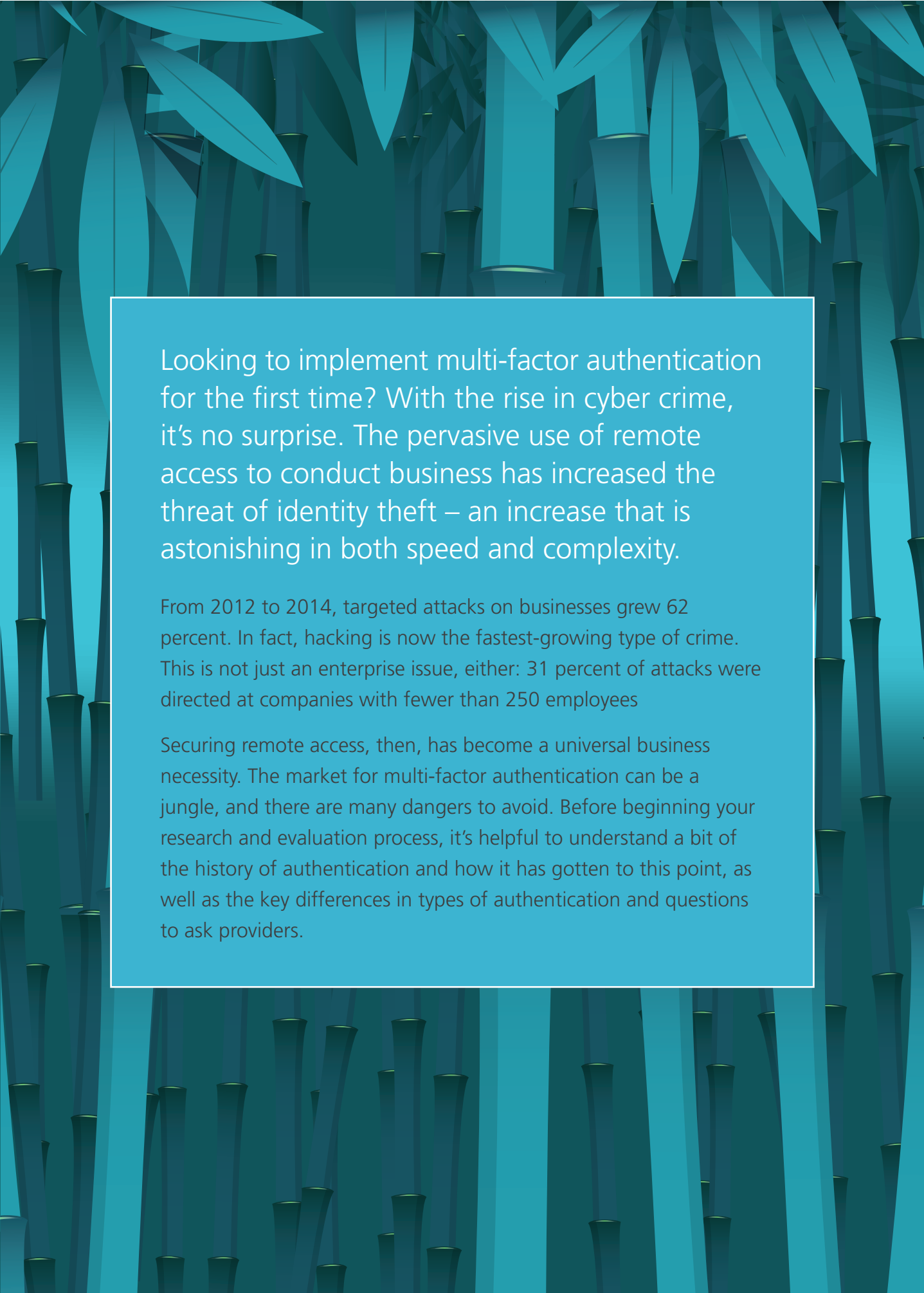


Whitepaper

THE BEGINNER'S GUIDE TO ~~TWO~~ MULTI-FACTOR AUTHENTICATION



YOUR GUIDE TO NAVIGATING THE JUNGLE OF
MULTI-FACTOR AUTHENTICATION SOLUTIONS



Looking to implement multi-factor authentication for the first time? With the rise in cyber crime, it's no surprise. The pervasive use of remote access to conduct business has increased the threat of identity theft – an increase that is astonishing in both speed and complexity.

From 2012 to 2014, targeted attacks on businesses grew 62 percent. In fact, hacking is now the fastest-growing type of crime. This is not just an enterprise issue, either: 31 percent of attacks were directed at companies with fewer than 250 employees

Securing remote access, then, has become a universal business necessity. The market for multi-factor authentication can be a jungle, and there are many dangers to avoid. Before beginning your research and evaluation process, it's helpful to understand a bit of the history of authentication and how it has gotten to this point, as well as the key differences in types of authentication and questions to ask providers.

WHY PASSWORDS ARE NO LONGER ENOUGH

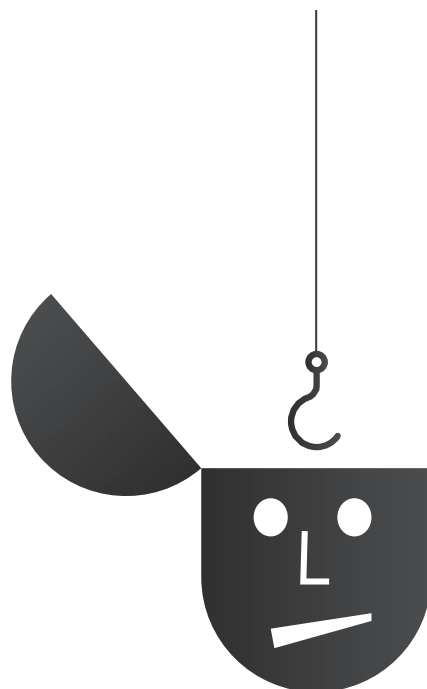
It's stunning to learn that 76 percent of all network breaches involve weak or stolen passwords. How is this possible, since passwords were created to act as a front-line identity defense?

Just as the use of cloud and mobile devices has evolved, so have threats and their complexity. In the early days of online services, usernames and passwords were typically the only form of authentication. To crack them, hackers used 'brute force' attacks to either guess the username or password, or 'dictionary attacks' to assume a user's identity. In a dictionary attack, a computer or a hacker attempts various combinations of potential passwords until access is granted.

In response, systems began to lock accounts after several bad attempts. Hackers then developed new techniques like key loggers.

Today, some of the most widely used attacks are pharming, phishing, pass-the-hash, or a combination of such methods. These terms describe methods by which users are led to an imposter website that looks identical to the original. This tricks the user into entering his or her username and password.

Some of the more advanced attacks send stolen information to the hackers in real time via a small instant message program, compromising many popular two-factor authentication tokens. As an example, Zeus malware captures a user's credentials – even advanced time-based token codes – and sends the information to the hacker. Yet many organizations are unaware that traditional hardware tokens can be compromised, posing a significant security risk.

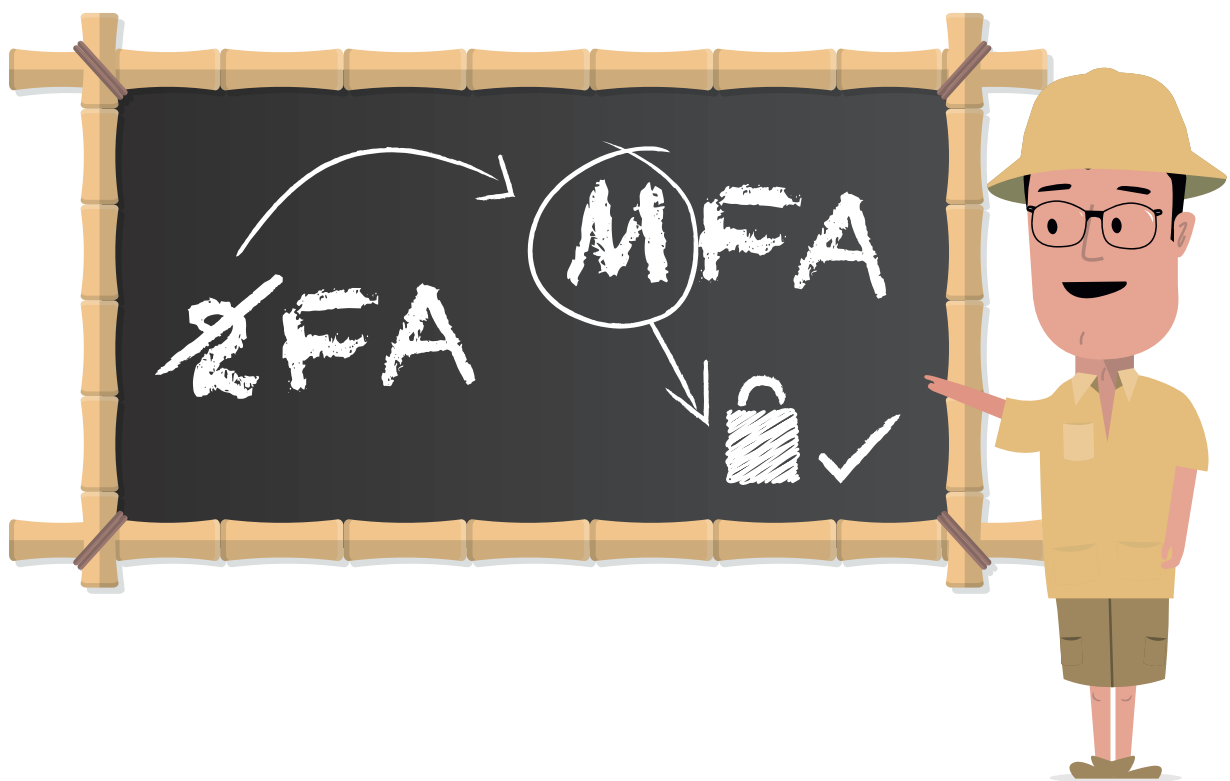


76%
**NETWORK
BREACHES
INVOLVE
WEAK OR
STOLEN
PASSWORDS**

2FA VERSUS MFA: WHAT ARE THE DIFFERENCES?

Two-factor authentication (2FA) and multi-factor authentication (MFA) are not synonymous and, as mentioned above, do not offer the same level of protection. 2FA is based on something you know (password) and something you have (a token, card, fingerprint, phone etc.). This method protects against threats that originally appeared in the '90s, such as key loggers and passwords that were guessed, cracked, bought or borrowed. MFA simply adds more factors to validate a user's identity. These can include your connection (unique session

identification), your geographic location, the role or rights you have as the member of a group, a valid point of entry and the time of day. However keep in mind that this is not simply a matter of having as many factors as possible in play when authenticating users. What is important is which factors are used and the context they are used in to identify the user. For example, capturing the GEO-IP of the user is not relevant unless this information is used actively in determining trust around the login.



THE EVOLUTION OF USER AUTHENTICATION TECHNOLOGY

25 years of strong user authentication can be described in three phases:

1 1990's – HIGH-RISK SEGMENT

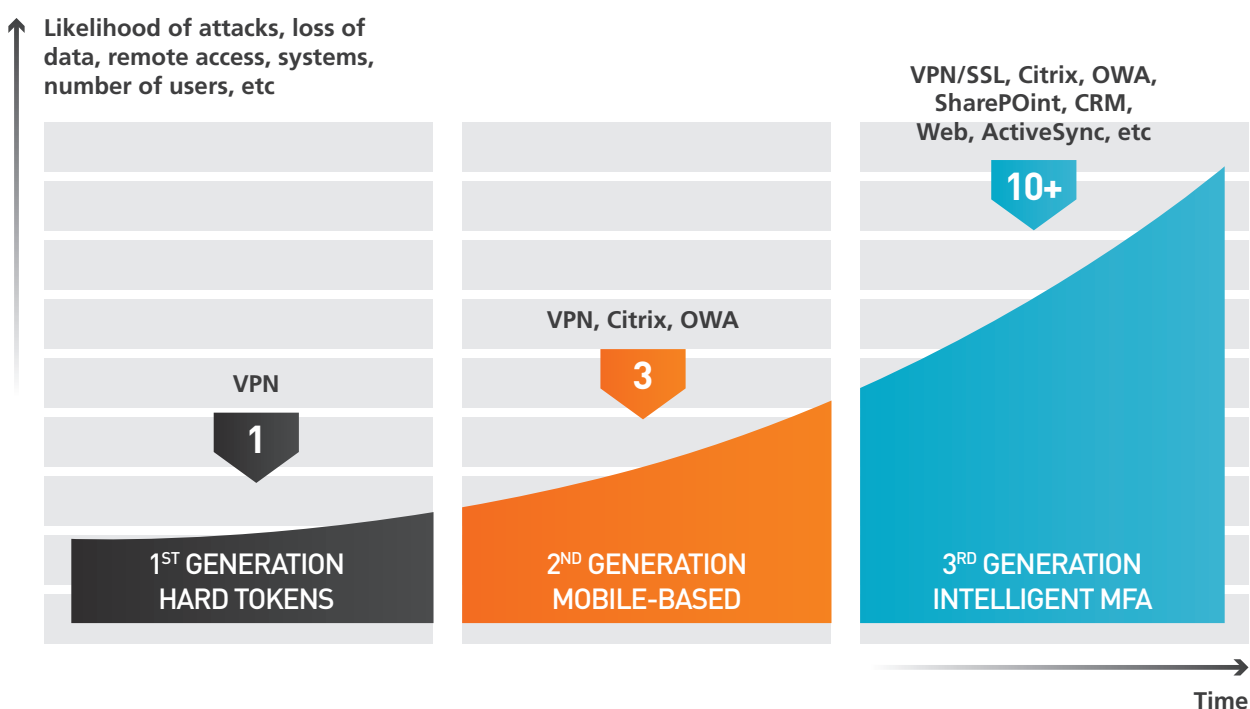
Financial and government institutions, in particular security-oriented branches of government, put hardware tokens into use. They were the early adopters of two-factor authentication. This segment typically had only few people accessing one or more systems remotely, so deploying hardware tokens was not a big burden to IT.

2 2000's – ENTERPRISES

Larger organizations across all industries realized the need for more security and mobile-based, two-factor authentication became a best practice. Remote access became available to more employees and more systems were accessed remotely i.e. VPNs, Web Access, Citrix, etc.

3 2010's – EVERYONE ELSE

Hacking has become a frequent part of the news cycle. Ransomware and APTs pose big risks. Keyloggers and other malware are dispersed across the net, and everyone has become a target. This has necessitated the evolution from two-factor authentication to intelligent multi-factor authentication. Remote access to data is critical, not just for white collars, but also blue collars, external consultants, etc. and there are many entry points that need to be protected. Enterprises increasingly demand authentication solutions that offer hardened security, are convenient for the users, and are easy to deploy, manage, and scale, allowing their business to remain agile and productive.



HOW TO PICK THE RIGHT SOLUTION FOR YOUR BUSINESS

The need for multi-factor authentication is clear, but knowing how to find the right solution for your organization may not be.

Navigating the market for multi-factor authentication can be tricky. With so many vendors to choose from, and so many different approaches, how do you find the solution that is right for your business? To help you we have put together an evaluation checklist that you can use as a blueprint for finding the right solution for your business.

With this checklist you will have all the right questions to ask a security vendor, so you can navigate the jungle of multi-factor authentication solutions.

We have grouped the checklist into these three key categories:



Will it protect my business against modern cyber threats?



Will it be easy to deploy, manage, and scale?



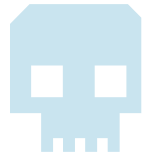
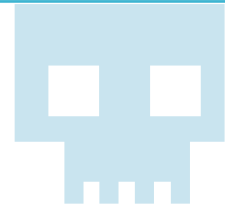
Can I trust and depend on this to work in the real world?

SOLUTION CHECKLIST



WILL IT PROTECT MY BUSINESS AGAINST MODERN CYBER THREATS?

You need the best defense possible to keep your data safe. Below questions will help you identify the less secure solutions that no longer provide the level of security needed to safeguard against modern cyber threats.



	YES	NO
1 Does the solution generate one-time-passcodes (OTPs) in real-time?	<input checked="" type="radio"/>	<input type="radio"/>
2 Does the solution depend on a seed file of any kind?	<input type="radio"/>	<input checked="" type="radio"/>
3 Does the solution use pre-issued passcodes?	<input type="radio"/>	<input checked="" type="radio"/>
4 Are OTPs sent out-of-band?	<input checked="" type="radio"/>	<input type="radio"/>
5 Are OTPs locked to the individual login session-ID?	<input checked="" type="radio"/>	<input type="radio"/>
6 Is the solution challenge-based to help block against DoS and Brute Force attacks?	<input checked="" type="radio"/>	<input type="radio"/>
7 Does the solution benefit from contextual information like GEO-location, time, and login behavior to determine the level of trust around each login?	<input checked="" type="radio"/>	<input type="radio"/>
8 Does the solution enable you to increase security via GEO-fencing?	<input checked="" type="radio"/>	<input type="radio"/>
9 Does the solution notify the users automatically if their passwords have been compromised?	<input checked="" type="radio"/>	<input type="radio"/>

SOLUTION CHECKLIST



WILL IT BE EASY TO DEPLOY, MANAGE, AND SCALE?

You need a solution that is easy to deploy, manage, and scale, and can support you in the future as your business grows and more systems need to be protected.



	YES	NO
1 Does the solution require you to deploy certificates?	<input type="radio"/>	<input checked="" type="radio"/>
2 Does the solution depend on deployment of software to the users mobile phones, laptops or other devices?	<input type="radio"/>	<input checked="" type="radio"/>
3 Does the solution depend on manual deployment of any kind, e.g. hardware tokens?	<input type="radio"/>	<input checked="" type="radio"/>
4 Does the solution integrate seamlessly with Microsoft ActiveDirectory?	<input checked="" type="radio"/>	<input type="radio"/>
5 Does the solution offer a self-service portal for end-users to adjust their preferences?	<input checked="" type="radio"/>	<input type="radio"/>
6 Does the solution require any AD schema extensions?	<input type="radio"/>	<input checked="" type="radio"/>
7 Can you scale and extend the infrastructure on-the-fly?	<input checked="" type="radio"/>	<input type="radio"/>
8 Will you need additional databases to store user information?	<input type="radio"/>	<input checked="" type="radio"/>
9 Does the solution allow for a flexible policy-driven administration of your users?	<input checked="" type="radio"/>	<input type="radio"/>
10 Does the solution integrate to all your remote access systems?	<input checked="" type="radio"/>	<input type="radio"/>
11 Can the solution secure your cloud applications?	<input checked="" type="radio"/>	<input type="radio"/>

SOLUTION CHECKLIST



CAN I TRUST AND DEPEND ON THIS TO WORK IN THE REAL WORLD?



You need a solution that users can depend on anytime and anywhere.

		YES	NO
1	What happens if an OTP does not arrive, does the solution have automatic failover mechanisms in place?	<input checked="" type="radio"/>	<input type="radio"/>
2	Does the solution provide you with analytics that allow you to interpret login data and identify possible threats?	<input checked="" type="radio"/>	<input type="radio"/>
3	Is the solution intuitive and hassle-free to use for the users?	<input checked="" type="radio"/>	<input type="radio"/>
4	Does the solution require training of the end users?	<input type="radio"/>	<input checked="" type="radio"/>
5	Are OTPs stored on the users phones?	<input type="radio"/>	<input checked="" type="radio"/>
6	Does the solution offer adaptive authentication that adapts the level of security based on trust at the point of login?	<input checked="" type="radio"/>	<input type="radio"/>

FINAL SCORE:

21-25 correct answers – This is the type of solution you should be looking at for a strategic solution that will support your security, administration, and convenience requirements now and in the future. If less than 25 correct answers then think carefully on what compromises you are making.

15-20 correct answers – This solution is not a good match, and you are adding significant risk to your business if you proceed.

0-14 correct answers – Don't go there.

GETTING AUTHENTICATION UP TO SPEED

The Internet's black market means big business for cyber criminals who relentlessly steal personal and corporate data. Many organizations are still relying on the 20-year-old technology behind two-factor authentication for protection, but as has been shown, 2FA is not up to the challenge. Modern threats require a modern authentication approach, specifically one that can deliver a session- and location-specific code to the user's mobile phone in real time.

I hope these questions help you understand what to look for and what to ask vendors so you end up with the right solution for your business. A solution that protects your business against modern threats, will be easy to deploy, manage and scale, and that you can trust and depend on 24/7.

It's a jungle out there, but with this guide your path to success is clear. Good luck in your search.



ABOUT THE AUTHOR



Claus Rosendal is a founding member of SMS PASSCODE A/S, where he oversees the product strategy and development in the role of Chief Technology Officer. Prior to founding SMS PASSCODE A/S, he was a co-founder of Conecto A/S, a leading consulting company within the area of mobile computing and IT security solutions with special emphasis on Citrix, Blackberry and other advanced handheld devices. Prior to founding Conecto A/S, he headed up his own IT consulting company, where he was responsible for several successful ERP implementations in different companies (C5 / SAP). Claus holds a Master Degree in computer science from the University of Copenhagen.

HUNGRY FOR MORE?

For a more detailed explanation on what makes a strong multi-factor authentication solution, we recommend these guides:



The Hidden Dangers of 'Good Enough' Authentication Solutions

<http://info.smspasscode.com/hidden-dangers-of-good-enough-authentication-solutions>



The Ultimate Guide to Token-free Authentication

<http://info.smspasscode.com/token-free>

To learn more about SMS PASSCODE, visit
www.smspasscode.com