TechVision RESEARCH

Multi-Factor Authentication (MFA): Enterprise Strategy and Market Assessment

Published 25 January 2019

Abstract

Multi-Factor Authentication is gaining traction as a best practice for enterprise security programs. It is based on the premise that traditional, single factor authentication schemes (like IDs and passwords) are relatively easy to break and as threats escalate, simply not good enough. It is a good time to consider making MFA a cornerstone of your enterprise IAM infrastructure given improved MFA vendor offerings and the inherent weaknesses of phishing-vulnerable password-based authentication. Requiring multiple factors from different categories for high risk or high value transactions is the emerging security best practice standard.

A great MFA strategy consists of utilizing multiple sources of identity along with a set of business rules and information that can dynamically identify the degree of certainty of a user's identity, while also being convenient to the user.

This report starts by looking at the basic components and use cases for MFA, then evaluates the types of MFA approaches currently being deployed, the impact of MFA on the enterprise and provides a review of our short-list of vendors and solutions. We also leverage our consulting experience in providing a pragmatic checklist or starting point for organizations looking to architect, prototype, build/source and deploy an MFA solution for their enterprise. We then conclude with a set of recommendations and next steps.

Authors:

Doug Simmons
Principal Consulting Analyst
dsimmons@techvisionresearch.com

Gary Rowe
CEO / Principal Consulting Analyst
gary@techvisionresearch.com

John Myracle
Principal Consulting Analyst
jmyracle@techvisionresearch.com

Sorell Slaymaker
Principal Consulting Analyst
sorell@techvisionresearch.com

Table of Contents

Executive Summary

Multi-factor authentication (MFA) is one of the most active and important areas within information security and IAM today. For well over a decade, the use of passwords to authenticate has been suspect; in particular for high value transactions the use of simple, relatively insecure and often recycled, easily guessed or stolen passwords are not good enough. To be sure, one of the most sought-after pieces of personal identifiable information (PII) is the username and password; this is especially problematic in that individuals often reuse the same username/password combinations at multiple sites. Requiring other factor(s) to access valuable content or to conduct high-value transactions is increasingly required and is the focus of this report.

Multi-factor authentication is a subset of the authentication market and is often evoked based on adaptive authentication or step-up authentication based on security policy and/or contextual data regarding the person requesting access. The challenge with MFA is to balance the need for security with ease of use. This balance is supported by the execution of policies that build on reliable contextual data to dynamically determine when MFA is needed and when single factor authentication is sufficient.

Measuring the degree of certainty that a user is who they say they are will increase as more data from more categories are collected. The more data that are collected in support of the user's request across the four ranges of what a person knows, who they are, what they have, and their history—the greater the degree of certainty. This is the basis for multi-factor authentication.

MFA is critical in the area of fraud prevention, and identity theft is one of the most prevalent and harmful forms of fraud in existence today. Over the past few years, significant advancements in the ability to deploy MFA to wide ranging constituencies – from employees, contractors, business partners to customers have made it much more palatable for enterprises of all sizes and types to consider.

With the advent of mobile device ubiquity and the willingness for end users to deploy apps on these devices, techniques such as 'mobile push' have gradually broken down the barriers of cost and complexity to deploy MFA. With that said, it is a good time to consider making MFA a cornerstone of your enterprise IAM infrastructure and start saying goodbye to the inherent weaknesses of phishing-vulnerable password-based authentication. Furthermore, as we begin re-architecting our enterprise environments to incorporate elements of Zero Trust, MFA becomes a critical piece of the ZT-puzzle.

TechVision Research has been espousing the notion of 'identity as the new perimeter' for the last several years. Within this concept, it is actually "identity + device" that becomes the perimeter. In a ZT environment, the most critical facet of security is knowing who (or what) the end user is as well as the device being used to authenticate that user or thing. This is the new perimeter; this combination of coupling an identifier with something the user has with them (like a mobile phone). Without the appropriate deployment of MFA, the authentication function remains one of the – if not *the*, weakest link in the enterprise and it is incumbent upon the enterprise security leadership to close this gap.

While other, more 'legacy' types of MFA such as One Time Password (OTP) tokens and smart cards still have a place in the IAM ecosystems for certain high-risk environments such as defense, finance, health-care, and IT administration, they can be considered deprecated in most enterprise situations. That is not to say they are no longer needed, but in many instances, the new age of mobile device-based MFA is more convenient and sufficient in many use cases to improve identity verification upon system login. Caveats to be considered of course include the actual ubiquity of mobile devices and network coverage/reliability in your environment – but in most cases, these caveats are in the minority.

In this report, we provide a checklist to help you gauge your readiness and can go a long way toward ensuring that you've prepared your lines of business and your infrastructure for deployment. Like all things IT: the better you prepare, document your use cases and 'user stories', involve your key stakeholders, select the right vendor/tool for the mission and roll-out your services in a controlled, well-governed manner – the better your chance for success. Critical to enterprise success is the ability to measure levels of identity assurance and to do anomaly detection of abnormal access attempts.

With that as the backdrop, this report identifies the leading business drivers effecting MFA adoption in both the enterprise and consumer-facing use cases, reviews the various types of MFA available, provides best practice insights for MFA deployment and reviews a short list of vendors who are leading the MFA revolution with their offerings. In short, we are looking to provide practical advice and guidelines for architecting, designing, building and deploying your future-state MFA program.

Introduction

Cyber threats are becoming increasingly sophisticated and include a variety of techniques that involve guessed, hacked, or physically or virtually stolen credentials. These threats expose the inherent weakness within traditional username/password-based authentication schemes. Accounts that have been compromised can create even greater damage as individuals use the same credentials, or a limited pool of credentials to authenticate and access services across multiple sites. Increasingly elaborate large-scale data breaches are directed towards extracting replicated/repeated login credentials.

What is needed is a means to mitigate the sharing of usernames and passwords and limit damage if they are compromised. Integrating Multi-factor Authentication (MFA) as a secondary or even tertiary security measure requiring an 'out-of-band-channel' to complete authentication. MFA makes it harder and more expensive for bad actors to compromise an organization.

Bad actors can gain access to user names and passwords by:

- Brute Force – Phishing thousands of users, hoping one will make a mistake
- Targeting – Going after a specific user and trying to brute force guess their username and password, getting an associate to divulge this information, video surveillance such as a hidden camera or using their smart phone to record you logging in. Keystroke loggers fit into this category
- Purchase – Buying user information from bad actors such as an electronic health record that has personal information such as a user's social security number, address, phone number, work place, health procedure and emergency contacts

The greatest risk of stealing someone's account information is in the process of creating or modifying the account, especially password resets, change of physical address or change in mobile phone number. Enterprises should ensure that extra steps in support of identity protection are taken when account information is being modified.

In light of these threats and attacks, organizations are positioning multi-layered authentication as a fundamental capability for increasing the protection of digital assets and TechVision believes this is a prudent strategy. The pervasive approach is to integrate a second and 3rd security layer employing additional factor(s) before authenticating and/or providing access to resources as defined within enterprise security policies.

As more and more people interact in the digital world through online banking, online healthcare and education, remote enterprise access and so forth, they often need to submit highly sensitive personal or financial information via the Internet. Given this effect, the need for ensuring data privacy and protecting personally identifiable information (PII) has also become critical.

Data privacy has become the focus of the international community and is reflected in the various governmental data protection laws and privacy regulations. From a regulatory perspective, the legal obligation to ensure compliance with all of these laws is left for interpretation by an organization's Legal Counsel. In short, even when viewed outside of the international body of

governing privacy law, virtually *every organization* has some level of data privacy and protection responsibility. Preventing unauthorized or unintentional (e.g. accidental and fraudulent) access or release of an employee's, customer's or patient's financial, health, and other forms of confidential and sensitive PII or business information is a key strategic security underpinning. Providing access security measures at multiple-layers at an infrastructure and policy-level will be needed for complying with future privacy initiatives. These privacy initiatives continue to advance, build, and evolve, at state, federal, and international levels.

In summary, there are a number of factors driving the need for adding additional levels of security to the existing logon credentials currently in use. They include enterprise goals of:

- Ensuring that the user or thing is who they say they are,
- Facilitating equitable and reliable access for all employees, business partners or customers from anywhere,
- Preventing unauthorized access to sensitive enterprise data ranging from trade secrets to an individual's account commensurate with protections postulated by Risk Management,
- Preventing unauthorized or unintentional release of sensitive corporate data and individuals' personally identifiable information, financial data, and other stored data, and
- Satisfying the organization's dedication to the goal of protecting its data and ensuring privacy.

What is MFA

Multifactor authentication can be defined as the use of more than one set of credentials from multiple categories that are used in concert to better determine (hopefully unequivocally) that you are who you say you are. Typically, one category of 'factors' is something that you know, such as a user ID and password. A second factor that is added to this is often something that you have, such as a smart phone, smart card, token fob or other such unique device that when paired with the first factor (something that you know), increases the veracity of authentication. A third factor can be incorporated as well – something that you are. Biometrics typically fill this bill with digital representations of your face (facial recognition), fingerprint, retina scan or voice print. Fourth is something that you have done. This can include where you have logged into from before (IP network address), recent transactions, time of day, last password reset, and flags for multiple failed login attempts

To be clear MFA includes a minimum of two factors from at least two of the following four categories; 1) something you know, 2) something you have, 3) something you are, and 4) something you have done. It is often invoked when there is a high value transaction or there is a

risk of a breach, but it's overall use is increasing. The risk profile could be raised based on activities such as multiple password attempts, the use of a new browser or the detection of a new geographic location not previously associated with the user.

While most systems and services still use the traditional user ID and password combination (i.e., single factor authentication) as the primary means to access online systems, this is rapidly changing as most enterprises are (and should be) examining stronger authentication approaches including MFA.

While most systems and services still use the traditional user ID and password combination (i.e., single factor authentication) as the primary means to access online systems, this is rapidly changing as most enterprises are (and should be) examining stronger authentication approaches including MFA.

The Continuing Evolution of MFA

It has been recognized for the past few decades that single factor authentication was often a risk, especially when the user is accessing sensitive applications and data. The use of MFA was limited especially in working with customers/prospects (note that even a single factor is often too hard to remember given the multitude of sites in which individuals are asked for ID/Password credentials). The widespread use of single factor authentication given usability concerns about more complex solutions has created barriers that have limited, or at least delayed, the widespread adoption of MFA.

Two relatively popular mechanisms for deploying MFA – or at least 2FA over the past thirty years are 1) Public Key Infrastructure (PKI) with smart cards using X.509 certificates and 2) Keys or one-time-password (OTP) tokens that functioned as the second factor. These approaches provided the something you have (smart card or keys/OTP), in addition to a user ID and password or personal identification number (PIN). While these two popular approaches were relatively successful in raising the authentication veracity bar, they were (and still are) expensive and complex to deploy and can be difficult to use. Plus, these methods do not guarantee 100% user identification. Many enterprises add MFA and then get lazy. For instance, if a bad actor gets the user name and password, and then calls the help desk to get a new OTP token.

To scale MFA and gain the associated security benefits the industry requires a more pervasive solution across a broad user base that is less expensive, easier to use and simpler to deploy. The good news is that we are getting closer to 'MFA for the masses' as we'll cover in the vendor section later in the report. The confluence of mobile phone adoption along with along mobile applications that communicate with enterprise MFA servers, provide the ubiquitous platform for serving up one-time 'password codes' or to facilitate biometric integration like facial, fingerprint and voice recognition. This is ushering in a new breed of MFA solutions from both startup vendors and large industry platform providers including Google, Microsoft, DUO Security and Authy – to name just a few.

As we describe the evolutionary path towards pervasive MFA in the following sections, be aware that there is still no magic pixie dust that allows MFA to be deployed without a well-thought-out strategy that weighs the risks, costs and usability. The good news is that we are moving in a direction in which MFA is more cost effective and deployable across a broad spectrum of use cases – both internal enterprise and consumer-facing. But an enterprise MFA strategy must consider the association between authentication cost and risk reduction as described in the following figure:

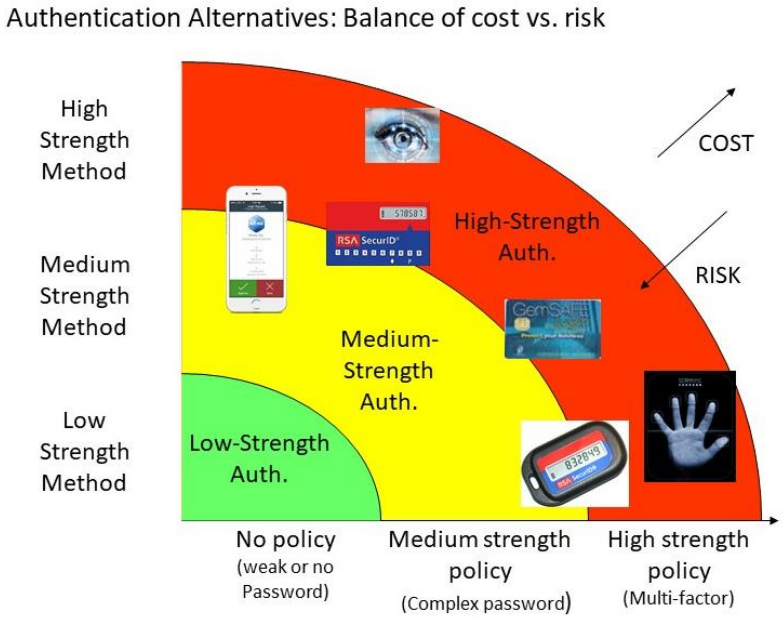

Figure 1: Enterprise Authentication Decision Points

Initial Identity Vetting

Before we get into the specifics of MFA, we need to start with an understanding of identity vetting, as evoking MFA on a suspect identity is like closing the barn door after the horses have escaped. Identity must be vetted before issuing credentials and is generally the first step towards establishing the requisite level of confidence that the authenticating user is in fact who they say they are. The appropriate level of identity vetting upon credential issuance is a key function of Enterprise Risk Management. In other words, the level of identity verification must be commensurate with the level of risk associated with the IT asset to be accessed. The strongest MFA technology could be deployed by an enterprise, but if the initial identity vetting process is weak, the entire authentication topology is weakened, as well. Please bear this fact in mind as we progress through this report and ensure proper attention is given to a strong vetting process. This may include initial in-person vetting with multiple forms of documentation for individuals that may be accessing high value assets.

We'll now look at how MFA has progressed over the years while understanding that many of the early technologies are still being actively used today. And, as we mentioned earlier, there are many organizations that don't even use MFA today for many use cases, but this is rapidly changing.

Early MFA; Token FOB for Remote Access

The primary early MFA approach was initially called two-factor authentication (2FA) and generally used a token FOB for remote access to systems via corporate Virtual Private Networks (VPNs). The pioneer in this space, starting in the mid-1990's was RSA with their SecurID 'token', a fob that generates a one-time password (OTP) periodically (e.g., every 30 seconds) and is synchronized with a remote access server (RAS) supporting the VPN. This rotating, synchronized password method makes OTP solutions impervious to replay attacks, which is one of the key vulnerabilities of the 'static' passwords so widely used. These solutions work with the end user using the one-time password provided by token fob to authenticate to the corporate VPN – along with their user ID and associated password.

This relatively simple method of enabling 2FA 'back in the day' worked wonders for many (primarily) large and distributed organizations. There are some factors that limited the impact of these early 2FA approaches as follows:

- Access to the VPN via 2FA didn't mean single sign-on to the corporate intranet – it simply let a person access the network. The applications running on the network would need to be integrated in order to support single sign-on via an application front-end such as a Web Access Manager (WAM) – which typically would only support User ID/Password.
- The token fobs were relatively expensive– typically in the $45 per user range, so it was a significant expense item and required additional scrutiny and corporate expense if they were lost (or stolen).
- The seed algorithm used to generate the synchronized one-time passwords on fobs and servers was not as secure as had originally been thought. In 2011, RSA's SecurID platform had been breached at Lockheed-Martin – a major U.S. Defense contractor. While this could have been truly catastrophic for RSA, they worked diligently to replace the fobs, better secure the seed algorithm and recommend to its customers that they beef up their own password policies to strengthen the security of the UID/PWD and OTP combination.
- Variations on the SecurID token fob theme have since emerged. For instance, Yubico offers a small USB token with an embedded chip that creates an OTP when a key is pressed and simulates a keyboard to facilitate easily entering a long password. Since it is a USB device it avoids the inconvenience of battery replacement. Additionally, versions of OTP technology have been developed that embed a keypad into a payment card of standard size and thickness. The card has an embedded keypad, display, microprocessor and proximity chip.

Soft Token OTP

As we said earlier, token fob OTP solutions (and virtually all these early MFA programs) have not gone away and are still in relatively widespread use today – particularly in higher security environments such as government defense contractors and similar entities. However, in the early 2000's it was recognized that the cost, deployment and management of hardware tokens in support of OTP were in many cases overly burdensome. In response, vendors such as RSA, Entrust, Gemalto and others developed software tokens that could be stored on general-purpose electronic devices such as desktop computers, laptops, or mobile phones. Because software tokens are something one does not physically possess, they are exposed to certain threats based on duplication of the underlying cryptographic material - for example, computer viruses and software attacks. Both hardware and software tokens are vulnerable to bot-based man-in-the-middle attacks, or to simple phishing attacks in which the one-time password provided by the token is solicited, and then supplied to the genuine website in a timely manner. Software tokens do have benefits over hardware tokens: there are no physical tokens to carry, they do not contain batteries that will run out, and they are generally less expensive than hardware tokens. Many enterprises have deployed 'soft tokens' as a way to improve authentication, but enterprises recognize and consider efforts to mitigate the potential threats we just described.

PKI Smart Cards

In the 1990's, PKI was expected to reach the masses. X.509 certificates issued to individuals holding credit card-sized smart cards that contained a cryptographic chip. Similar to OTP token fobs, the smart card constitutes something you have, and when authenticating to a system with a smart card reader, the card holder enters a PIN (something you know) to enable the authentication process. In a nutshell, the challenges with deploying trusted certificates to large numbers of end users, coupled with supplying card readers on virtually every desktop or laptop the end users would access was costly and complex. Cards were lost, certificates needed to be revoked and reissued, Certificate Authority (CA) servers were needed, certificate revocation lists (CRLs) maintained and so forth – leading to a slow adoption rate that has since petered out even more.

The Introduction of the Smart Phone

While vendors were making hay with the SecurID token fob and soft token approach of the day and the attempts at large-scale PKI smart card authentication continued, the world was quickly ramping up rabid adoption of smart phones. While earlier 'dumb cell phones' supported short message service (SMS) text messaging in the mid-late 90s and early 2000's, the advent of the iPhone and Google's Android mobile device operating system spurred the smart phone revolution and the term 'texting' became a household word. Secondly, cellular network providers were rapidly improving SMS reliability and range. The combination of these two factors brought the smart phone into the fold as a bona fide 'second factor' – or 'something you have' that could obviate the need for a specialized token fob OTP generator or smart card for many organizations. This sequence of events was the real harbinger for widespread adoption of MFA within organizations of all sizes as well as the consumer and e-commerce site interactions.

This wasn't lost on the financial community, as banks – needing to develop newer and more accurate ways to 'know your customer' (KYC) as mandated by regulatory groups guiding them, began to deploy MFA in the form of text messages with OTP 'codes' embedded in them to their customers' phones in order to enable a key second factor to the authentication process with online banking – your UID, password and the code just sent to your cell phone on record in your account profile.

This method of using SMS text messages to send OTP's to customers and enterprise users is still very much in vogue today. It mostly works and works well, with little up-front investment for the customer, employee or enterprise. It does, however, disregard those users who may – heaven forbid – not own or don't, at run time, have access to a cell phone. So, let's consider the '80/20 rule': if (at least) 80% of the users being addressed own a cell phone that can be reached quite readily from the OTP code generator, then the other 20% (or less) will have to be supported some other way. Often times, this is where the Security organization will mitigate risk by a number of additional defense-in-depth approaches. Generally speaking, the overall risk posture was improved – even with the 80/20 rule being considered.

The greatest risk is using a mobile device and associated SMS message is when this device is lost, stolen, or broken. In this case the user may still need access, but another method of authentication will need to be used. In the process of getting a new device, a bad actor can imitate a user. And that bad actor can leverage social media to gain insight as to when a user goes on vacation and can subsequently work with the help desk to get their credentials and send the SMS password to a different phone number. Thanks again to social media, data of birth, city of birth, high school, favorite pet or pet name, … is all available to add to the "something I know".

But the major phone vendors have helped support the MFA movement. For example, Apple released the Apple Push Notification service (APN) back in 2009 and less than a year later Google released its own Google Cloud to Device Messaging service (C2DM) for Android devices. A 'push notification' is a message that pops up on a mobile device. Push notifications look like SMS text messages and mobile alerts, but they only reach users who have installed an app on the device to receive the messages. Typically, the end user receiving the MFA push notification on his or her device must 'push' a soft button on the display that means they acknowledge the fact that they are logging into an online system. Because the person with the phone (something they have) must be the same person logging into the online system with their UID/password (something they know), the end result is 2FA. Simply adding the requirement to provide their fingerprint (something they are) to this process-whether within the push app itself or by virtue of the smart device's biometric capability, we can effectively deploy MFA.

This advancement in cellular messaging provided a big push (no pun intended) to make MFA much more user-friendly MFA. Along with Google and Apple, a new breed of MFA has vendor emerged; vendors that created MFA applications for iOS and Android devices as well as laptops running Windows and OSX. Companies like DUO Security and Authy quickly gained favor with enterprises in the MFA space because of the popularity of the tool with end users (including consumers) and relative ease of deployment and integration. Needless to say, legacy 2FA vendors like RSA adopted push technology in addition to their existing solution sets. Additionally, many IAM vendors that enable and support the authentication processes of their customers, such as Microsoft, ForgeRock, Okta, Janrain, Gigya/SAP and many others added push authentication capabilities to their products. As of this writing, the smart phone enabled push notification has emerged as the leading class of MFA solutions. While this approach isn't perfect for all situations and certain high-risk use cases, it is very user friendly and readily integrated.

the smart phone enabled push notification has emerged as the leading class of MFA solutions.

There are some challenges as sophisticated bad actors can change caller ID. Close associates can see a new SMS on your cellular device when you take a quick break without knowing your phone login code or biometrics. Thus, the enterprise strategy should start with zero trust and then grant least privilege access based on level of identity assurance (or probability).

Authentication Standards

Authentication standards are emerging and should be considered as a starting point for an enterprise MFA program. For instance, the Initiative for Open Authentication (OATH) addresses authentication integration challenges with standard, open technology that is freely available to application developers. OATH is a collaborative effort of IT industry leaders aimed at providing a reference architecture for universal strong authentication across users, devices networks. Through an open standard freely available to all, it is intended that OATH will offer more hardware choices, lower cost of ownership, and allow customers to replace existing disparate and proprietary authentication systems whose complexity often leads to higher costs. OATH's framework components are designed to be interoperable in solution development and deployment by enabling straightforward integration with existing identity and access management platforms and infrastructure (e.g. LDAP directories, web access management and single sign-on servers).

The OATH standard, at a basic level, describes implementation of a core set of authentication credentials. These credentials are:

- One Time Password (OTP) - based authentication
- Public key infrastructure (PKI) - based authentication (using X509.v3 certificate)
- Subscriber identity module (SIM) - based authentication (using GSM/GPRS SIM)

The OATH standard has been ratified in a series of IETF RFCs. Because OATH-based solutions can be compatible, migration between products is intended to become simpler and can leverage a much larger range of devices for OTP generation, such as YubiKey, and even sharing of hardware tokens between vendors. An important architecture goal for universal authentication is to enforce the separation between validation and identity stores. OATH recommends that all identities (user or device identities, as well as device-to-user bindings) be maintained outside the validation server. This separation is important from an integration and cost-control standpoint because it promotes a distributed architecture that favors the reuse of an enterprise's existing infrastructure (e.g., corporate directories). In such architectures, the validation server is a minimal front end. OATH assumes that LDAP (including Active Directory and Azure Active Directory) is used to enable the validation server and the directory to exchange information. The OATH standard is currently being contributed to by a large number of vendors, including Gemalto, HID, Symantec, VASCO, Yubico and many others (please see https://openauthentication.org/members/), and is supported by a number of MFA vendors (discussed in further detail later in this document).

Another important standard in the MFA arena has been developed and promulgated by the FIDO (Fast Identity Online) Alliance, an industry consortium launched in February 2013 to address the lack of interoperability among strong authentication devices (PayPal and Lenovo were among the founders).

FIDO's aim is to support a full range of authentication technologies, including biometrics, Trusted Platform Modules (TPM), USB security tokens, smart cards, and near field communication (NFC). FIDO specifications provide two categories of user experiences, depending on whether the user interacts with the Universal Second Factor protocol or the Universal Authentication Framework protocol. Both of these FIDO standards define a common interface at the client for the local authentication method that the user deploys. The client can be pre–installed on the operating system or web browser.

FIDO members totaled more than 260, including a Board made up of Aetna, Amazon, American Express, Bank of America, Gemalto, Google, Intel, Lenovo, MasterCard, Microsoft, NTT DoCoMo, PayPal, Qualcomm, RSA, Samsung Electronics, USAA, Visa, VMware, Yubico and many others.

As we have learned over the past few decades, end-users thrive on standards – they do a lot of good in terms of fostering interoperability, reducing vendor lock-in and facilitating integration. The problem with standards is that there can be too many of them, and sometimes this dramatically reduces their ability achieve these objectives. TechVision Research feels that OATH and FIDO are the two premier standards in MFA technology development and vendors that incorporate either or both of these standards are better suited for most enterprise customers.

TechVision Research feels that OATH and FIDO are the two premier standards in MFA

Biometrics and MFA

Biometrics is an important element of the "who you are" category. Remember that at least two factors from two separate categories are required for MFA; the what you know is typically the user ID/password, the what you have might be your phone or smart card and the what you are is often biometrics such as facial recognition, your fingerprint, retinal scan, voice print or something else that is part of the individual.

Biometric authentication has often been viewed as the 'holy grail' of MFA. Over the past three decades, there were numerous challenges in 'early' biometrics deployment and adoption topped by resulting in false positives and false negatives due to the early limitations of biometric readers and scanners. Given the recent investment, adoption and advancement of mobile device technology by vendors such as Apple, Google, Samsung, LG and many other smart phone manufacturers and operating platform providers, we have seen dramatic improvement in biometrics capability and reliability. Today, many MFA vendors can leverage the Trusted Platform Module (TPM) interface in these mobile devices to determine that the user had authenticated to their device via facial recognition or fingerprint biometrics and can incorporate this awareness into the overall strength of the end-to-end MFA session – leading to the elimination on the reliance of a user inputting a PIN (something she knows) and instead relying on biometric authentication to the mobile device as the second factor (something/who she is) in addition to possession of the device (something she has). Some biometric characteristics to consider are as follows:

Biometric systems can be spoofed, so they should be used in conjunction with other types of authentication.

- Voice biometrics works well if a user calls on a regular basis and there is a long sample history. Voice biometrics needs a quality connection so that the voice quality has a mean opinion score above 4.0. Voice biometrics systems will return a probability score on how well the voice heuristics match that of previous samples.
- Facial recognition works well for users signing into a device such as a phone, tablet, or kiosk. Recently, airlines such as Delta have added facial recognition to their self-service check-in kiosks to improve security and user convenience.
- Fingerprints are used for secure access to systems such as Clear for airport security entrance identification. Iris scanning is another example, but is less prevalent because of the inconvenience to users, especially those wearing contacts.
- Biometric systems can be spoofed, so they should be used in conjunction with other types of authentication. For instance, one can take 5 minutes of you tube video and create a voice or facial biometric print. We have all seen in the spy movies people chopping off fingers to get access to systems.

Future State of MFA

We have anticipated the demise of password-centric authentication for decades. Our position is that this future is now or at least rapidly approaching. For the reasons we have been discussing – device and network ubiquity, reliability, Bring Your Own Device (BYOD) initiatives coupled with the accelerating levels of fraud associated with password-based authentication, the time has arrived to deploy MFA in your enterprise.

As we discuss in greater detail later in this document, many large, influential vendors such as Microsoft, Cisco and others have laid down the gauntlet; they have drawn a line in the sand and have started shouting from the rooftops that the password is truly dead. Let's be clear – the replacement of password-based authentication is an evolutionary process, as most consumers likely used usernames and passwords to authenticate to their networks or sites this morning - but simple IDs and passwords are about to become yesterday's news – and fast. This is why every major enterprise needs to have a well thought out MFA strategy in place in 2019.

The shifting of major IT infrastructures to the cloud via SaaS, PaaS and IaaS provide the opportunity to reinvent authentication – and that is what is happening. If your organization is migrating to Azure, there will come a time within the next 18-24 months when passwords are deprecated. Furthermore, as the concepts associated with Zero Trust continue to evolve and take hold, MFA will be an imperative.

Will there be advancements over the next 3-5 years beyond mobile devices acting as the 'something you have' factor? Probably, but it won't just be a more advanced phone as that factor; it could be your car, your watch, your house or many other "things" that haven't yet been invented. There are a wide range of future combinations of things that can become MFA enablers – including biometrics that can be plugged into MFA. The key to being ready for this future is to start the journey now.

About TechVision

World-class research requires world-class consulting analysts and our team is just that. Gaining value from research also means having access to research. All TechVision Research licenses are enterprise licenses; this means everyone that needs access to content can have access to content. We know major technology initiatives involve many different skill sets across an organization and limiting content to a few can compromise the effectiveness of the team and the success of the initiative. Our research leverages our team's in-depth knowledge as well as their real-world consulting experience. We combine great analyst skills with real world client experiences to provide a deep and balanced perspective.

TechVision Consulting builds off our research with specific projects to help organizations better understand, architect, select, build, and deploy infrastructure technologies. Our well-rounded experience and strong analytical skills help us separate the "hype" from the reality. This provides organizations with a deeper understanding of the full scope of vendor capabilities, product life cycles, and a basis for making more informed decisions. We also support vendors in areas such as product and strategy reviews and assessments, requirement analysis, target market assessment, technology trend analysis, go-to-market plan assessment, and gap analysis.

TechVision Updates will provide regular updates on the latest developments with respect to the issues addressed in this report.

About the Authors

Doug Simmons brings more than 25 years of experience in IT security, risk management and identity and access management (IAM). He focuses on IT security, risk management and IAM. Doug holds a double major in Computer Science and Business Administration.

While leading consulting at Burton Group for 10 years and security, and identity management consulting at Gartner for 5 years, Doug has performed hundreds of engagements for large enterprise clients in multiple vertical industries including financial services, health care, higher education, federal and state government, manufacturing, aerospace, energy, utilities and critical infrastructure.

Gary Rowe is a seasoned technology analyst, consultant, advisor, executive and entrepreneur. Mr. Rowe helped architect, build and sell two companies and has been on the forefront the standardization and business application of core infrastructure technologies over the past 35 years. Core areas of focus include identity and access management, blockchain, Internet of Things, cloud computing, security/risk management, privacy, innovation, AI, new IT/business models and organizational strategies.

He was President of Burton Group from 1999 to 2010, the leading technology infrastructure research and consulting firm. Mr. Rowe grew Burton to over $30+ million in revenue on a self-funded basis, sold Burton to Gartner in 2010 and supported the acquisition as Burton President at Gartner.

John Myracle is a technical specialist/architect with a broad technology and diverse business background. Mr. Myracle combines knowledge of intellectual property with product conceptualization development and delivery. Experience includes communicating business, financial, and technical objectives between legal, sales, marketing, and development teams for banking, communications, optical transport network management, security, mobile, and medical device applications. Patent experience includes drafting 150+ applications and IP portfolio monetization.

Mr. Myracle is a seasoned system/solution architect, product manager, and senior consultant with 35+ years' experience at Booz-Allen & Hamilton, IBM, and Southwestern Bell Corporation. Core focus areas range from cloud computing and IoT to European Union GDPR compliance and smart contracts on blockchain.

Sorell Slaymaker has 30 years of experience designing, building, securing, and operating IP networks and the communication services that run across them. His mission is to help make communication easier, cheaper and more secure since he believes that the more we communicate, the better we are. Prior to joining TechVision Research, Sorell was an Evangelist for 128 Technology which is a routing and security software company. Prior to that, Sorell was a Gartner analyst covering enterprise networking, security, and communications.

Sorell is an IT Architect with a focus on network, security, and communications architecture. He specializes in IT Architecture – Network Architecture, SIP Trunking, Contact Centers, Unified Communications, and Security Architecture.