WHITE PAPER

Advanced Authentication Buyers Guide

Introduction

What is advanced authentication and its relationship to zero trust and the journey to passwordless?

Advanced authentication goes beyond basic 2fa and multifactor authentication by adding risk-based factors and enabling complete coverage through current and emerging standards based protocols.

The zero trust model is identity centric and demands accurate identity verification only attainable through a MFA architecture. While passwords will probably be around for a while longer, attaining a high security passwordless environment is the ultimate goal. Advanced authentication is the first step.

The bottom line: Adopting multi-factor authentication prevents the most common attacks on corporate networks. Advanced authentication goes a step further toward the higher security, greater convenience of a passwordless environment.

As organizations move to adopt advanced authentication, the challenge lies in selecting a solution that addresses their unique requirements and covers all authentication use cases. This document was created to aid you in your selection of an advanced authentication vendor and help ensure that your choice is the right one for your organization.

ADVANCED AUTHENTICATION SOLUTION SELECTION CRITERIA

The following sections identify criteria to use in your vendor evaluation process.

1. Completeness of Solution

It is common for enterprises to have complex IT environments incorporating a wide variety of platforms and applications, both old and new. Left unsecured, these assets (including PCs, mobile devices, servers, thin clients, VPN clients, Windows applications, cloud applications and even green screen mainframe applications) are potential targets of cyberattacks. Leaving even one of these systems without protection could compromise your entire network.

Unfortunately, many products on the market offer only basic 2fa protection. In the face of today's diverse enterprise environment, it is critical to select an authentication vendor that provides complete coverage for all your corporate assets. Before you engage vendors, take an inventory of the applications and platforms required to be secured by multifactor authentication. This step will become an invaluable tool when later assessing the breadth of coverage provided by any advanced authentication solution under consideration.

Also consider all potential use cases for authentication in your environment. In addition to the platform and application considerations above, it's important to understand the use cases that are critical to your enterprise.

2. Ease of Implementation

The principal barriers to multifactor authentication adoption have been the cost and disruption that such projects frequently entail. Rolling out multifactor authentication solutions could quickly balloon into complex projects lasting from months to years,

consuming prodigious amounts of critical IT resources that are expensive and in short supply. The exorbitant time and resources needed to deploy many MFA or SSO solutions are driven by weighty solution requirements, such as fork-lift system upgrades, application modifications, new server installation and configuration, provisioning and end-user training.

When selecting a multifactor authentication vendor, insist on a full disclosure of the implementation requirements and consider solutions with the following attributes:

- Can be deployed in a matter of days instead of months
- Integrates with legacy architectures as well as emerging cloud models
- Retains investment in systems and processes
- Doesn't require the installation and management of new, dedicated servers
- Doesn't require code changes to existing applications
- Requires little to no end-user training

3. Administration and Management

Installation and provisioning are just the first hurdles in adopting a multifactor authentication solution. Administration and maintenance can be equally daunting, taxing already overextended IT personnel and requiring security skills that are expensive and hard to find.

Examining the components integral to most authentication solutions makes it clear why many organizations have balked at adoption:

- Additional dedicated servers to manage
- New administrative consoles and UI to learn
- Ongoing synchronization and management of multiple user stores
- New and complex authentication workflows that result in helpdesk calls from end users

However, administering MFA need not be an ordeal. Asking a few questions upfront when evaluating a solution will save you money, conserve precious IT resources, and avoid chronic IT staff and employee frustration. For example:

- Does the solution require new data center hardware?
- Can I manage all devices, applications and user stores centrally?
- Are there new system interfaces to learn and master?
- What end-user self-service capabilities does the solution provide, such as password reset?

4. Standards based APIs and emerging technology

As previously mentioned, complete coverage of all IT assets across distributed, diverse systems, is a requirement of the modern enterprise. It is important that the advanced authentication solution fit into the current IT architecture, security policies and preferred authenticators as well as provide a path forward. For example, the advanced authentication solution should continue to evolve in step with enterprise cloud migration strategies.

Leveraging industry authentication interface standards and technologies ensures interoperability with diversified systems and applications. Just a few notable examples include:

- SAML - Security Assertion Markup Language (SAML) is an open standard that allows identity providers to pass authorization credentials to service providers. This makes it simpler to use one set of credentials to log into many different websites.

- Active Directory Federation Services (ADFS) - a software component developed by Microsoft, it is commonly used to provide users with single sign-on access to systems and applications located across organizational boundaries.
- Azure Active Directory (Azure AD) - Microsoft's cloud-based identity and access management service.
- FIDO - The FIDO protocols use standard public key cryptography techniques to provide strong authentication.
- PKI – Leverages a standard public key infrastructure to enable organizations to centrally create, manage, use and revoke digital certificates.

By leveraging standards your authentication vendor can provide ease of integration into current IT system, enable SSO across distributed IT systems and applications, ensure investment protection as your enterprise evolves into new IT architectures and adopts emerging technologies.

5. Breadth of Authentication Factors

Enterprises are faced with an ever-growing mixture of endpoints, users, geographies and applications, all of which have varied risk profiles and capabilities. IT security administrators need the widest possible spectrum of authentication options, allowing them to choose the strength of security based on the type of transaction and the authentication factors appropriate to the endpoint. No single type of credential is a "magic bullet." Solutions with a rich and varied set of authentication methods used individually or in combination provide the flexibility to tailor policies based on an organization's unique security environment, industry best practices and regulatory mandates.

Many solutions on the market today provide a narrow set of authentication factors that may constrain your ability to establish a comprehensive and strong authentication posture and potentially leave serious security holes. Consider vendors that provide a full palette of authenticators from each of the well-known authentication categories:

- Something you have: Smart, Proximity and Contactless Cards; Bluetooth Phone; OTP
- Something you know: PIN, Password
- Something you are: Biometrics
- What you do: User behavior analytics
- Where you are: IP address, GEO location
- When you act: Time

A special note on biometrics is in order. The adoption of biometrics has seen a steep uptake over the past several years, and for good reason. In addition to being a strong credential, it is the only authentication factor that provides "Proof of Presence" or non-repudiation. In short, biometrics provides a best practice method for knowing who did what, when. This kind of visibility injects accountability into authentication workflows and establishes a strong barrier to credential theft. Unfortunately, many vendors include biometric authentication as an afterthought. Biometrics is an exacting science that requires deep domain experience. During vendor assessment, scrutinize the vendor's core biometrics expertise. They should have a solid history of delivering best-in-class biometric systems across all industries and use cases.

6. Single Sign-On

Single Sign-on has seen an increased adoption by enterprises of all types in order to provide an improved user experience and increased productivity. A typical user accesses a large number of IT resources during the course of a working day. SSO simplifies the authentication process, allowing users to sign in once and subsequently access all their applications, transparently. There are many other benefits that SSO affords, such as:

- Facilitating definition and enforcement of uniform authentication policies
- Improving auditability and security reporting
- Freeing developers from having to implement authentication per application
- Reduceing help-desk costs due to password resets
- Allowing for instant revocation of access rights for terminated users

In addition to the authentication factors enumerated above, look for solutions that include SSO federation as an integral part of their offering.

Average cost of
SINGLE PASSWORD RESET

7. Converged Access Control

The rise in innovative and smart building technologies has created a growing need for converged physical- and network-based access controls. The infrastructure of an existing intelligent facility is such that it can easily be a host of elements, such as cloud, remote access, and data sharing and analysis, as these become crucial in reaping the benefits of a connected and converged space.

Physical Security and IT departments are recognizing that now, more than ever, converged threats are real. Vulnerabilities that exist in both domains are fronts that have traditionally been handled separately. In isolation, they can be viewed as managed risks. But when malicious attacks or simple carelessness connect these vulnerabilities, the risks become more than the sum of their parts.

To meet the growing security needs of today's organization, Physical Security and IT are aligning their objectives to reduce risks while ensuring convenience for employees. While more converged physical and logical access technologies can help show the way, the ultimate responsibility lies within security professionals to chart the right course for their organization.

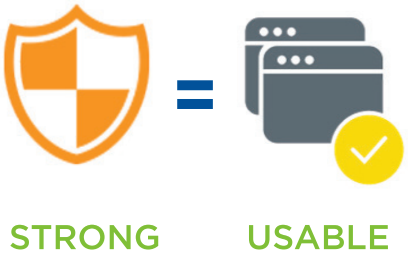
Physical access architectures can be quite complex and include mixed varieties of technology and multiple vendor components. Enterprises may consider an advanced authentication vendor that is both well versed at managing complex PACS systems as well as converging the gap to IT system authentication. One of the quickest and easiest places to start is with a converged credential such as a smart card or a fingerprint scan used for both physical access and logon to IT systems.

8. Administrative Accounts

While it is important to secure all user accounts with access and authentication polices, special attention should be given to those with administrative privileges. Whether an authorized "privileged" user inside the organization or an external hacker posing as one accesses data, the potential danger each poses remains the same—unauthorized destructive or fraudulent activities. With their system-level access rights, privileged users can wreak more havoc than any other class of user and need elevated levels of security to mitigate the risk they pose. To protect yourself from these potential bad actors, it is vital to authenticate their identities with multifactor authentication and audit their activities in order to shut down illicit activities before damage occurs. As you are evaluating authentication solutions, look for those that provide a uniform way to secure both privileged and non-privileged user access, making deployment and management easier.

9. Security Architecture

In the past, organizations have adopted multiple point security solutions based on discrete use cases. The problem with this approach is that as the number of disjunct solutions increases, the difficulty and cost of maintaining them skyrockets. Adopting multiple security systems, usually proprietary in nature, also makes responding to new security threats and new use cases difficult because of their inherent lack of extensibility. Going forward, solutions that incorporate a broad range of authentication factors into one single architecture based on open standards provide the best option for building an effective layered security infrastructure now while allowing organizations to respond to future security threats as they arise. Not only will this approach yield better



security results, it will also reduce the cost of administering security systems, decrease infrastructure costs, and ultimately reduce the total cost of ownership. As you evaluate advanced authentication solutions, consider those that also accommodate third-party or standards-based authentication methods in addition to the vendor's proprietary ones. Optimally, the vendor will provide API's to extend their solution to incorporate additional platforms, applications and authentication methods, freeing customers from proprietary lock-in. Give special consideration to the following points when selecting a solution:

- Native support for target platforms or applications, such as Microsoft Credential Provider and smart card infrastructure
- Tight integration with industry standard directories, such as Microsoft Active Directory and Lightweight Directory Service
- Direct integration into systems and applications via a vendor supplied API
- Protection for keys, credentials and processes in a manner which is at least as secure as the host
- Integrated, policy-driven central management of all authentication methods
- Central IT control of all policies and authentication events
- Simple policy management by Group or Application
- Centralized management using familiar Microsoft tools
- Visibility into all authentication events to detect anomalous activity and report usage

10. Ease of Use

For an advanced authentication solution to be successful it must be easy to use. Users will be inclined to adhere to easy-to-use authentication methods that minimally impact workflow.

The best approach is to select an advanced authentication solution that provides a wide array of authenticators with varying usability attributes, allowing you to tailor authentication requirements in accordance with transactional risks. The solutions should allow IT security administrators to step up authentication for high-risk authentication transactions and simplify authentication workflow for lower-risk ones.

Ease of use can also be achieved through a consistent authentication workflow across platforms and applications. This is another reason to seek solutions that integrate a wide variety of authentication methods under a common architecture, with a common user interface.

When it comes to users ease of use is accomplished by enabling authentication tokens that they are either already familiar or otherwise natural to use. For example, most employees of medium and large enterprises are familiar with using a smart card or smart ID badge to gain access to buildings and other physical assets. In this case it may make sense to use the smart card to log into IT systems as well. Using a dual purpose security token also enables evolution toward converged access control.

Mobile applications are something all employees are accustomed to using in their daily lives. Using secure mobile authentication on mobile devices can be easy to deploy and quickly adopted by users.

Fingerprint readers and facial scanners are cheap, portable and easy to integrate as a means of authentication. Fingerprint and facial authenticators make it particularly easy for users to present their biometrics for scanning. It does not even take user consciousness, just a casual scan and you are done.

The use of elements from the categories of something you HAVE, something you KNOW, and something you ARE drives effective multifactor authentication. In a properly designed authentication framework, biometrics can be used to unlock and enter random system-generated cryptographic material, eliminating the need for users to ever create or remember passwords.

Further, when using a biometric, such as a fingerprint, the key is not sharable and can't be lost or forgotten. Biometrics provide a highly usable form of authentication, resulting in greater user acceptance and adherence to authentication policies.

It is important to select a solution that provides a wide portfolio of authentication factors. Vendors should be evaluated based on their experience in delivering highly usable, secure systems to diverse markets and applications, as well as the seamless and secure integration of biometrics into existing and evolving IT architectures.

11. Scalability

As businesses grow, their IT systems need to scale to support increased workloads while maintaining expected performance levels. Yet, despite its importance, scalability is poorly understood. Simply put, scalability is a measure of a system's ability to provide increased throughput, reduced response time, and/or support more users when hardware resources are added.

Often times, the words performance and scalability are used interchangeably, but the two are distinct: performance measures the speed with which a single request can be executed, while scalability measures the ability to maintain performance under increasing load. Achieving linear scalability means maintaining performance as workload increases by adding more machines, CPUs or memory, without changing application code.

Ultimately, scalability is a system property. If the system is not designed to use additional resources to maintain performance under increasing load, it will not be scalable.

When evaluating authentication solution vendors, make sure to ask them to share their system models with you. Their models should map performance against workload and show how increasing CPU, memory or server resources affects system performance. They should also be able to provide hard data on how to configure their solution to accommodate varying workloads, especially those with high daily peak loads.

12. Adaptability

The modern enterprise consists not only of internal constituents but an expanding list of third-party vendors, service providers, suppliers and independent consultants. To enhance business agility, these third-parties have been integrated into the enterprise network, but in the process have become one of its biggest security exposures. Indeed, many of the recent data breaches have been laid at the doorstep of these partner organizations due to lax security practices. A network is only as secure as its weakest link, and the weakest link has proven to be the many partner companies that comprise the extended supply chain. It is critical for enterprises to ensure that best security practices be extended throughout their entire supply chain. To achieve this, multifactor authentication solutions need to easily adapt to include partner access controls, using the same methods deployed inside the enterprise network. Partner access and authentication controls should not require separate authentication systems with all the additional complexity and cost such duplication would entail. The evaluation of advanced authentication solutions should include an assessment of their ability to adapt and protect the entire supply chain using the same authentication factors, interfaces and management practices.

13. Extensibility

Security threats to the enterprise network are continuously evolving. Cyber criminals don't give up and go home when security countermeasures are brought online. Instead, they adapt to enterprise security systems, searching for and finding new exposures to exploit. To be viable over the long-term, authentication vendors need to rapidly extend protection against new threat vectors and incorporate the latest security technologies into their solutions.

Always ask vendors to demonstrate how their product has evolved and provide a future roadmap. This is the best way to evaluate their agility and responsiveness to emerging threats and ultimately, their viability as a security vendor.

14. Flexibility

Just as the security landscape is constantly morphing, the authentication needs of organizations also change. Mergers and acquisitions, new markets, changes to IT infrastructure, evolving compliance mandates and new end-user devices and operating systems can all change the authentication needs of the enterprise. In the face of a rapidly changing business environment, multifactor authentication solutions need to provide flexible deployment models and allow IT security administrators to change the mix and types of authentication factors quickly and efficiently as the need arises.

Vendors that integrate a diverse and complete array of authentication factors within their architecture using open standards and industry best practices are best able to respond to the changing needs of enterprise customers. With such an architecture, organizations can set up their authentication infrastructure to use a mix of factors—and change their mixture as conditions change.

15. Portability

The age of mobility is upon us. This is nowhere more apparent than in the global dispersion of enterprise workers. Mobile workers need to be able to conduct business:

- From any location
- From any device
- At any time
- Whether they have a network connection or not

Authentication solutions need to support all these mobile use cases with authentication methods that are tightly integrated into their core authentication architecture. Be sure to ask vendors to explain how they support the mobile work force, especially as they pertain to your specific mobile use cases.

16. Compliance

As mentioned above, businesses are under increasing regulatory pressure, which requires them to continually monitor and control access to enterprise resources based on granular policy definition. Compliance not just a good idea, it's the law. Failure to comply with governmental and industrial mandates can result in crushing fines at best and criminal charges at worst.

To facilitate compliance, an authentication solution should provide the following capabilities:

- IT security staff should be able to centrally define role-based access rights and apply authentication policies to protect and govern access to all corporate platforms, applications and data assets.
- The authentication solution should enforce all access and authentication policies.
- Access and authentication events must be logged and securely stored such that no one can alter them.
- IT security administrators must be able to run compliance reports for periodic compliance audits.

To assure that an authentication solution will meet your compliance needs, ask your prospective solution provider to share sample compliance reports with you.

VENDOR EVALUATION

Choosing the right advanced multifactor authentication vendor is probably the most important decision you'll need to make during your product selection process. You will be putting the security of your business in their hands and entering into a long-term, collaborative partnership. Creating a structured evaluation process replete with questions about their history, market presence, position and differentiation, customer successes, business practices and support capabilities is critical to making an informed and successful decision.

1. Company Focus

Does the company market a large portfolio of products, or is it tightly focused on advanced authentication and access management solutions?
A portfolio company might have spread itself thin with their many solution offerings, resulting in shortfalls in service, development resources and domain knowledge. If you are interviewing a portfolio company, consider the following areas of disclosure:

- Ask them to provide financials that disclose their major revenue centers. Is strong authentication one of them?
- How is support staff allocated across their portfolio?
- Ask about the tenure of their development and support staff. Does it appear that there is high staff turnover, or are they able to retain top talent and create a depth of field expertise?
- Find out what their typical product release cycles are. Are they nimble and responsive to market needs and changes?

A company with a laser focus on IAM might provide a better choice. An organization that exclusively provides advanced authentication solutions has the luxury of dedicating development and service resources and aligning Sales and Marketing functions in service to the multifactor authentication needs of their customers. Such a singular focus enables the company to achieve and maintain a deep level of expertise in an industry characterized by rapid change and upheaval. At the other extreme are vendors with such a narrow focus that they only cover a limited number of use cases or only provide partial coverage of platforms and applications. Committing to such a vendor could leave you searching for solutions to plug the gap later. At that point, your choice is to either find and manage another supplemental vendor or rip out the original solution and find a vendor that provides full coverage. Both options represent wasted time and resources. It is best to carefully itemize your authentication requirements and find a vendor that can address all of them and has the resources to see you through implementation and beyond.

2. Company Size

Choosing a vendor of the right size is a bit of a Goldilocks decision. A company too small might not have the bandwidth to provide an acceptable level of service and support, nor be able to maintain development momentum as new threats and technologies arise.

A large vendor might be tuned to servicing high-revenue customers to the detriment of customers of lower financial value. Of course, this depends on the size of your company. If your company is itself large and represents a significant revenue flow to the vendor, a large company might suit you just fine.

The "just right" category includes mid-sized vendors that have achieved market traction and financial stability. These companies are focused on growth and are hungry for your business. They also have built out their development, service and support capabilities and have well developed, mature processes.

Whatever your criteria or preferences for vendor size, the provider you choose should be considered for their long-term commitment to your success and their ability to support your comprehensive authentication needs now and in the future.

3. Field Tested & Proven

Companies whose products have withstood years of rigorous use in the field have been hardened to a degree that just can't be matched by newer entrants. When selecting a product with a long history of market placement, you benefit from its years of learning and evolution. Companies that have long market experience also have a deeper industry understanding and are better able to anticipate your needs. Security is too critical a concern not to select fully mature companies with proven track records.

4. Solution Fit

Vendors that are heavily invested in selling their own products and technology can often times leave you with a solution that doesn't truly fit your needs. The first job of a vendor should be to sell you a solution that completely meets your requirements, instead of force-fitting their solution into your environment based on a biased and exclusive preference for their own in-house products. Solution vendors that are willing and able to extend their product offering with third-party technology in order to precisely solve your authentication challenges are preferable. Vendors in the best position to respond in this manner are those that, in addition to their proprietary technology, provide industry-standard interfaces and flexible API's that allow them to respond to unique customer requirements.

5. Global Presence

Companies with global presence need to know that their authentication vendor also has international offices. Look for a vendor with proven international experience and local service resources.

6. Service & Support

Before fully committing to a vendor, verify that they have a mature support organization with sufficient bandwidth to provide timely response to your service needs. Vendors of critical security systems need to offer highly effective support systems and staff to ensure that you derive full benefit from your security investment.

7. Professional Services

Every deployment is different, and every customer has unique needs. Make sure the vendor has world-class professional service offerings that can effectively resolve any deployment issues and make your rollout smooth and successful. The vendor should also have sufficiently advanced professional service expertise to adapt and tune their solution to your environment.

SUMMARY

Strong multifactor authentication is no longer an optional security investment. With the number and severity of data breaches due to compromised credentials splashed across the daily news, the question is not "if" your organization should deploy advanced authentication but "which solution" will meet your needs. There are a dizzying number of solution providers bringing new authentication offerings to the market. We hope this product selection guide will make selecting one easier, and that, when all is done, your organization can rest assured that its IT assets are secured to the highest degree possible.

hidglobal.com