Strong Authentication Buyers Guide

Introduction

The sheer number and destructiveness of data breaches in the past few years are alarming and discouraging. However, there is cause for hope. Most of these cyber attacks had a lot in common. One of the most alarming similarities in a majority of the attacks was the use of compromised credentials. Three-quarters of all breaches were largely due to weak or stolen credentials.

The good news is that the vast majority of security breaches could have been prevented by implementing and enforcing basic security best practices. Best practice recommendations for preventing security breaches come from every corner of the industry—analysts, consultants, governmental bodies and security organizations alike—and they speak as with one voice.

The consensus: Adopt strong multi-factor authentication to lock the front door and prevent the most common attacks on corporate networks.

As organizations move to adopt strong 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 a strong authentication vendor and help ensure that your choice is the right one for your organization.

STRONG 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 cyber attacks. Leaving even one of these systems without strong authentication protection could compromise your entire network.

Unfortunately, many strong authentication products on the market offer only partial 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 that must be secured with strong authentication. This step will become an invaluable tool when later assessing the breadth of coverage provided by any strong 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 multi-factor authentication adoption have been the cost and disruption that such projects frequently entail. Rolling out strong authentication solutions can 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 strong authentication 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 strong 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 or years
- Integrates with legacy architecture and applications
- 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 strong 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 strong authentication 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. Policy-based Access Controls

Employees need access to platforms, applications and data in order to fulfill their job responsibilities. However, security considerations and compliance mandates dictate that such access be granted based on the principle of least privilege: only provide access to assets that are essential to a user's job function. Further, user access to platforms, applications and data should be governed by authentication safeguards appropriate to and in accordance with the security risk those resources represent. Best practices in this case are to aggregate users into groups based on functional roles, map those roles to access rights, and apply appropriate levels of authentication to secure access.

These best practices are critical to adhering to compliance mandates such as Sarbanes–Oxley (SOX) and PCI DSS. Both of these mandates require that corporations implement access control based on carefully defined policies, maintain a secure audit log of all authentication events, and create audit reports for compliance auditors to inspect. Failure to do so can expose organizations to severe legal and financial penalties.

In consideration of the importance of policy-driven access controls, any strong authentication solution evaluated should include a comprehensive policy engine that will help define and document role-based access and authentication policies, enforce these policies, maintain a log of all access events, and subsequently provide reports for auditors. To ease the learning curve for creating policy-driven access controls, look for centrally managed solutions that leverage standard policy definition interfaces, such as Microsoft Active Directory.

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

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.

7. Password Management

Synchronizing and managing passwords across all enterprise platforms, applications and data stores can be time consuming and a major resource drain on IT departments. Unfortunately, this only accounts for a portion of the challenges that password management represents. In response to the recent onslaught of data breaches caused by compromised credentials, IT departments are increasingly adopting and enforcing strong password policies. Although the intent of such policies is to shore up security vulnerabilities, they frequently have the opposite effect, as end users cope with password complexity by writing them down—oftentimes on sticky notes in full public view. On the other hand, if employees dutifully create strong passwords and attempt to remember them, they usually end up forgetting them and call the help desk for a password reset. Gartner estimates that 20% to 50% of all helpdesk calls are for password resets, and, according to Forrester, the average cost of a single password reset is $70.

Average cost of **SINGLE PASSWORD RESET**

When evaluating strong authentication solutions, look for the following password management features:

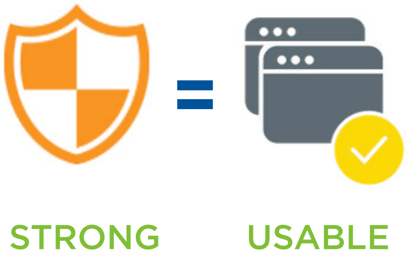
- Central management of passwords across all platforms and applications: The ability to centrally define password policies and propagate them to all systems will streamline the process, reduce errors, and relieve IT personnel from the time-consuming task of synchronizing multiple credential stores.
- Self-service password reset: Empowering end users to securely reset passwords should be a core solution requirement. This fundamental feature can eliminate password reset requests to your help desk, saving you considerable amounts of money.
- Automatic password generation and entry: The best way to remove the chronic problems associated with the use of passwords as a credential is to automatically generate and enter strong, fully random passwords on behalf of the user. This single feature can completely eliminate the primary security pitfall that has long plagued secure password selection —the inability of humans to create and remember strong, random passwords.

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 strong 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 strong authentication 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

Strong authentication methods can inversely affect usability, lowering productivity and causing users to search for ways to circumvent the system. Conversely, users will be inclined to adhere to easy-to-use authentication methods that minimally impact workflow.

The best approach is to select an 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 and centrally manage a wide variety of authentication methods under a common architecture, with a common user interface.

Chief amongst authentication usability challenges are those presented by passwords. In an effort to make passwords a strong authentication factor, IT organizations have instituted strong password policies. However, requiring users to select random, ten-character passwords containing a combination of letters, numbers and symbols for each application they need to access and then periodically change them has resulted in a usability disaster.

In an effort to deal with password overload, users cope by creating easy to remember passwords that, despite their best efforts, are easily crackable. Worse, they write them down as a memory aid and use the same one for multiple applications.

The fact is, passwords would actually be a strong authentication factor if the human element were removed. Today, there are ways of achieving this goal. Allowing the authentication system to generate strong passwords and automatically enter them into credential fields retains the benefits of passwords while avoiding their pitfalls. The best way to achieve this is through the use of biometrics.

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

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 strong authentication policies.

It is important to select a solution that provides a balanced portfolio of all three authentication factors, with biometrics playing a critical component. Vendors should be evaluated based on their experience in delivering highly usable biometric systems to diverse markets and applications, as well as the seamless and secure integration of biometrics into their solution offering.

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 forenterprises to ensure that best security practices be extended throughout their entire supply chain. To achieve this, strong 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 strong 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, strong 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

Strong 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 strong 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 strong authentication?

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 strong authentication might provide a better choice. A company that exclusively provides strong authentication solutions has the luxury of dedicating development and service resources and aligning Sales and Marketing functions in service to the strong 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 multi-factor 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 strong 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

2019-06-06-iam-strong-authentication-buyer-guide-wp-en

PLT-04529