Realtime publishers

The Essentials Series: Architecting the Right Solution for Strong Authentication

Selecting a Strong Authentication Solution

sponsored by

by Jeffery Hicks

Selecting a Strong Authentication Solution 1
Strong Authentication Myths and Misconceptions 1
Strong Authentication Is Too Expensive 1
Strong Authentication Is Too Difficult to Manage 2
Strong Authentication Impedes User Workflows 2
Strong Authentication Has a Low User Adoption Rate 3
Solution Requirements 3
Multi-Protocol Support 3
Easy Deployment and Management 4
Consolidated Reporting and Auditing 4
Meets Sector, Regulatory, or Compliance Requirements 4
Finding a Solution 5
Consult with Peers 5
Consult Industry-Trusted Publications and Resources 5
Find a Vendor with Clients and Case Studies in Your Industry 5
Evaluate and Test in *Your* Environment 6

Copyright Statement

Selecting a Strong Authentication Solution

Strong authentication solutions address many complex and difficult situations in today's corporate IT environment. But if these solutions are so terrific, why aren't they more widespread? If you want a solution, where do you begin?

Let me begin by expanding my definition of a strong authentication solution. This is more than simply installing a fingerprint scanner at every desktop, although that may be one part of it. Strong authentication solutions should interface with every system or resource that an employee or user interacts with, and it should do so with a minimal profile. I have a few other details for an ideal solution which I'll cover a little bit later.

Strong Authentication Myths and Misconceptions

If you ask any number of IT managers and systems administrators, you will likely discover a short list of excuses for not implementing a strong authentication solution. Oftentimes these excuses are really misconceptions, so let me clear away the clouds of confusion.

Strong Authentication Is Too Expensive

By far the number one myth and misconception is that strong authentication solutions are too expensive. I suppose if you are looking only at your shopping cart's total price, you might think so. However, you aren't simply buying a loaf of bread; you are making an investment in your IT infrastructure. You have to look at the full picture.

Let's start with security. With weak authentication, the risk of data loss or exposure is quite high. Depending on your industry, the consequences could be severe—from regulatory fines to civil actions to loss of customer goodwill. How much would a single data breach cost your company in hard dollars? I'm not even talking about the internal time and resources you will have to expend to deal with the situation. Oh, and don't forget about lost opportunity. While your company and employees are dealing with a security incident, they can't attend to other work, which means potential lost earnings.

Another hidden cost to weak authentication is the impact on user productivity. End users have to expend time managing passwords, calling the Help desk for password resets, or simply taking an extra few minutes to securely access a network resource. It may not seem like much but these minutes of lost productivity add up.

Let's say you have 100 employees and they spend 10 non-productive minutes a week dealing with the consequences of weak authentication. That's 1000 minutes a week of lost productivity. Multiply that by an average hourly rate of say $20 hour, which comes out to 33 cents a minute, and weak authentication is costing you $330 a week or over $17,000 a year! I haven't even factored in your IT costs to support all of this.

If you still aren't convinced, consider your auditing and reporting requirements to meet compliance or regulatory obligations. How much time are systems administrators or analysts spending collecting and compiling this information? How much time is spent formatting the data into an appropriate format? Are you confident that you haven't missed anything? What are the consequences if you have? The cost of IT goods and services should obviously never be ignored. However, don't neglect the "big picture," especially for an item that has the potential to affect every aspect of your organization's operation.

Strong Authentication Is Too Difficult to Manage

Often, companies believe that strong authentication solutions are too difficult to implement and manage. Although I won't say that there aren't solutions that might be more difficult compared with others, such a blanket generalization is self-defeating. One of your goals when selecting a solution is to identify one with a simple, easy-to-use management interface. You also want a solution that is seamless and unobtrusive. Perhaps in the past, early strong authentication solutions were complex and difficult to use, but they don't have to be.

If anything, a strong authentication solution should simplify the administrator's workload. Instead of a hodgepodge of management tools and procedures, s/he only has to learn how to use a single, comprehensive tool. Granted, some individual components of your strong authentication system may have their own management interface, but you should seek out products that allow you to consolidate and integrate.

Strong Authentication Impedes User Workflows

Another common misconception is that a strong authentication solution impedes user workflow. That is, it is merely an obstacle that prevents a user from getting his or her job done. IT professionals are concerned that end users will be confused by new security requirements and that having to authenticate, perhaps with biometrics, will take too long and disrupt productivity. Or suppose a company has adopted two-factor authentication with smart cards and the user leaves the card at home?

I'm not naïve enough to suggest that strong authentication will never impede a user's daily routine. However, proper user education and well-documented policies and practices should more than mitigate any losses. Don't forget that one of the downsides of weak authentication is the amount of time a user has to spend dealing with passwords and clumsy security implementations. If anything, weaker authentication is more of a hindrance, which the proper strong authentication solution can address.

Strong Authentication Has a Low User Adoption Rate

One final misconception is that users, and to some extent organizations, have been slow to adopt strong authentication solutions. In my opinion, this situation is a self-fulfilling prophecy. Companies are faced with many myths and misunderstandings surrounding strong authentication and consequently are slow to implement a solution, if they ever do. So yes, there may be a slow adoption rate, but that's only because of misinformation that dissuades many people.

The other contributing factor to this misperception is security itself. For many organizations, their security infrastructure remains confidential, and rightfully so, for many reasons. You can never truly know how many strong authentication solutions have been implemented in your area or industry sector, but working with the right vendor can help alleviate this worry.

Solution Requirements

Hopefully, I've convinced you by now regarding the viability and benefits of a strong authentication solution. Of course, like any product, not every solution is equal. The following sections explore key elements I think you should consider as requirements for any strong authentication solution.

Multi-Protocol Support

Consider your environment. How many different authentication systems and protocols are currently deployed? Do you have a physical access control system (PACS)? If you are in the healthcare sector, you might have a vertical application such as Siemens Medical. Do you employ a user provisioning system such as IBM's Tivoli Provisioning Manager? Or perhaps you are in the financial sector and rely heavily on a Fiserv solution? You need an authentication solution that can easily incorporate such an application. These are simply a few major technologies that come to mind; I'm sure you can identify many more in your company.

Your requirement for a strong authentication solution is to integrate all user access activities across multiple and disparate systems from physical access to network security. This has the effect of providing a comprehensive security infrastructure by integrating physical access with IT and data access. *Comprehensive* is definitely the key word here, followed closely by *seamless*. You require a solution that does not force you to cram it into your network with 20-page implementation checklists. You should be able to point the solution in the right direction and it does the rest.

Easy Deployment and Management

Which brings us to the next requirement you should seek: Any strong authentication you consider should be easy to deploy and shouldn't require an army of consultants or vendor technicians. Remember, you are looking for a solution that can fit seamlessly into your existing network and support multiple protocols and platforms.

One sure-fire test is to investigate what it takes to *remove* the solution. If uninstalling requires massive server reconfigurations, driver uninstalls, service account deletions, or system reboots, it more than likely is not a seamless solution and is far from unobtrusive.

Some solutions may require agent installation around your network. I've always felt the use of agents is personal preference. There is not anything inherently wrong in using agents, but they should be extremely easy to deploy and configure, consume a low amount of system resources, and otherwise maintain a low profile.

One of the end results from implementing strong authentication is that you want to make it easier to manage and control who gets access to corporate networks, applications, resources, and data. Very often, this includes password policy management.

Your preferred solution should have an easy-to-use management interface that consolidates all your disparate platforms. I'm personally fond of Web-based dashboards that I can securely access from anywhere. But a reasonable desktop application that doesn't require dedicated resources or hardware is acceptable as well.

Consolidated Reporting and Auditing

One of the primary reporting purposes for a strong authentication solution is to provide insight into all user access activities across the entire enterprise. This includes physical as well as IT services. The key word here is *comprehensive*. You need to be able to reliably report what resources a user accessed, where those resources were accessed, and when they were accessed. Reporting should be easy without requiring extensive work on your part to develop complex database queries or reporting templates.

> **Note**
>
> I hope it goes without saying that all of this data must remain secure and that access to this data is also monitored.

Meets Sector, Regulatory, or Compliance Requirements

Much of what we face in IT today, especially when it comes to regulatory requirements or compliance is *accountability*. Have you taken prudent and reasonable measures to protect data and network resources and can you prove it? I can only assume that you are aware of regulations and requirements that pertain to your sector or industry. You need to seek out a strong authentication solution that meets, or ideally exceeds, those requirements.

For example, in a healthcare setting, it is not uncommon for multiple users to share a common desktop. Often, these computers are in publicly accessible areas. Thus, the first step is to prevent unauthorized access without adding unnecessary steps for doctors, nurses, and technicians who legitimately need access. One solution might be a proximity card reader that authenticates the user who needs only enter a PIN.

However, even within this scenario, there is another layer. We've controlled access to the network but what about data? A lab technician needs access to specific parts of a patient's record. A physician waiting to use the same desktop needs access to the full patient record. Your strong authentication system should seamlessly authenticate the doctor's access to the data with minimal effort on her part. Of course, all of this is logged and easily reported.

Finding a Solution

Once you have identified your requirements for a strong authentication solution, it's time to go shopping. I have some advice that should streamline this process.

Consult with Peers

I can't think of a better recommendation than from a professional colleague whose opinion I trust. The first step I would take would be to contact my peers and discover what solutions they are using or even have considered. Granted, their environments will have different requirements, but you should still be able to narrow your list.

Consult Industry-Trusted Publications and Resources

Does your industry or sector publish trade-related journals or magazines? While there's nothing wrong with considering a vendor based on a trade advertisement, use caution. Typically, you only see the big players who have an advertising budget. There is no guarantee they have the expertise or experience to meet your needs. To compensate for this fact are there sector-related web sites that offer unbiased product information and reviews? This type of information is very valuable because these resources will be evaluating solutions based on your specific sector needs. A financial services organization will have different strong authentication requirements than a manufacturing company.

Find a Vendor with Clients and Case Studies in Your Industry

I think it is vital that you identify a vendor with clients similar to your own company. Or at the very least, they should offer related case studies. You wouldn't use a mechanic that specializes in brake repairs when you need transmission work. You must find a vendor with the experience and expertise to meet your requirements. The solution you are looking for has business-critical and enterprise-wide implications, so you can't afford a vendor who doesn't "get" your industry and requirements.

Evaluate and Test in *Your* Environment

Finally, the most important recommendation I can make is to evaluate and test in *your* environment. You need to understand what impact the solution has on your network, resources, and users. The right solution should be unobtrusive and easy to install as well as remove. Pilot test the solution with a representative cross-section of users and administrators. Provide the proper level of training and then evaluate the impact on their daily routines. Does the solution interfere with or enhance their daily routines? Can administrators easily manage everything? Do the reporting features meet your requirements? How responsive is the vendor when things go wrong?

This is not a process that you can complete in a few days or even a week. If I was the IT manager, I would be planning at least a 30-day trial and evaluation, especially if the company has end-of-month activities. You want to ensure that all business operations are supported. It is also critical to dedicate sufficient resources to properly manage and test everything during the trial period.

If all goes well, that is, users and administrators report a positive experience, you should be able to scale out the implementation and deploy enterprise-wide. In the final article of this series, I'll discuss concepts surrounding deployment and management of your strong authentication solution.