A NETIQ **FLASH POINT** PAPER

Multifactor authentication:
Removing risk while simplifying processes

Passwords are dead—again

The old way of thinking—using username and password to authenticate users—just isn't working any more. Why? There are several reasons. Users are careless with passwords. They choose ones that are obvious; they use the same password for every situation that requires one; and often times they even write them down at their desk. But it isn't all user error.

With username and password being the only requirements for access, you're providing hackers with an authentication model that they're used to cracking. Savvy criminals write advanced algorithms to find ways of entry. Then, when the same password is used across multiple situations, a hacker who has breached your security can make their way into other levels of access. Imagine: A hacker steals one of your user's Facebook passwords and in doing so obtains access to your entire corporate infrastructure.

The bottom line? With username and password, the entire authentication transaction is based on something a user has to know. And that something can be captured or stolen.

The conversation has shifted to multifactor authentication (MFA)

As the name suggests, MFA combines multiple identity sources as a means of access. But not just several identity sources. The best ones combine different ***types*** of identity sources. In the ideal situation, MFA combines two out of three things: Something you ***know***, for example a PIN code, with something physical that you ***have***, such as a key card or a token, and something you ***are,*** such as a fingerprint, a retina scan, or voice recognition. By requiring two of these three identity sources, you greatly reduce the risk of security breach.

CONDITIONS THAT MIGHT DRIVE THE DECISION TO IMPLEMENT MULTIFACTOR AUTHENTICATION:

- *Mandates*
- *Breach*
- *Technology/ infrastructure update*

The best MFA relies on responses to at least two of the following factors:

- **Something you know**
- **Something you have**
- **Something you are**

Technically, when your bank asks you for your PIN and also for your social security number, that may seem like MFA because it is two separate identity sources (one from the bank, one not from the bank). And while that may be true, it isn't a very sophisticated scenario, because both are things that you ***know***.

As a concept, it isn't new

It's the implementation that is new. MFA is something most people already use every day. At an ATM machine, you physically ***have*** a card and you ***know*** your PIN number. When checking in to most travel kiosks at the airport, you must both swipe your credit card (something you have) and enter the three digits of your destination city (something you know) in order to proceed. Even showing a photo ID in order to complete a credit card transaction (where the photo provides the "something you are" authentication) is multifactor.

It's clear why MFA is so valuable. Any system that requires two separate forms of authentication is inherently more secure, because it forces breaches to be location based. It isn't enough for a hacker to sit in Eastern Europe and grab usernames and passwords—they have to also be able to acquire (or spoof) the thing you ***have*** or the thing you **are**. Something not easily done.

What is making MFA a trend?

More and more organizations are becoming increasingly aware of the risk and cost associated with single-factor authentication of online transactional accounts. It's a costly trend that can be reversed with MFA, making electronic payments as quick and reliable as cash payments.

"Verizon's 2013 data breach report, which pointed the finger at single-factor authentication as a primary culprit in security spills, reported that 76 percent of network intrusions in 2012 exploited weak or stolen credentials ."

Another factor that is leading the charge for MFA is the onslaught of new government regulations and mandates, such as HIPAA. On March 26, 2013, new U.S. Department of Health and Human Services rules went into effect, extending HIPAA security and privacy requirements to business associates—which include contractors, vendors, and service providers, such as billing companies—that perform services on behalf of a health care provider or who provide solutions that integrate with medical or patient data. With hefty fines for non-compliance, many organizations are looking toward MFA to help them protect access to medical and patient data.

Last but not least is the fact that biometric authentication has been built in to many devices for quite a while now. With fingerprint scanners on smartphones and PCs, many businesses have had the capability to implement MFA for a while, they just haven't realized it or bothered to do it.

If MFA is so great, why haven't we been using it all along?

As with most advancements, the resistance to change is varied. Most companies aren't aware that they already have the components necessary for MFA (such as fingerprint scanners). There is also a concern about implementing something that will complicate user experience. Often, ease of use equates to efficiency, and organizations are hesitant to sacrifice workflow for any reason—even security. And lastly, but perhaps most importantly, in order to get the full benefit of MFA, you need to set up and optimize the access system on the back end. If you can't handle the information that comes in and implement it across the system, the benefits you receive are less than ideal.

It's time to change the thinking around MFA

When new technology gets rolled out, it often fails because nobody thought through all of the implications. For MFA, there are several things you need to consider before you start:

- Don't think of authentication as an ad-hoc acquisition or an embedded part of one element of your security system. Think about and establish your own advanced authentication policy
- Map out all of the places that MFA is going to be used (do keep in mind, if MFA is your access policy, you should probably use it). Try to eliminate complexity where you can by making MFA:
  - Easy to manage. The last thing you want is to be managing a bunch of different authentication systems for every different system in your company.
  - Easy to use. If it is hard to use, you'll get resistance. Very seriously consider implementing a single sign-on solution at the same time. This will preclude users from having to remember a bunch of different passwords or having to re-authenticate for every system.

Done right, MFA should actually make life easier for your users. After all, swiping your finger across a scanner and entering a PIN is easier than remembering a username and password.

Things to look for in an MFA vendor

Because implementing MFA is critical to supporting your security and productivity initiatives, it needs to work well with the way your business operates.

1. **Look for solutions that give you choice and flexibility in the kinds of authentication you require as well as how you apply it.**
2. **Don't let yourself get locked in to a single kind of physical authentication (in other words, don't let the hardware you choose dictate your authentication philosophy).**
3. **Look for vendors who develop to an open framework that is aggressively updated as new technologies are launched.**
4. **And finally, look for vendors who can make the system easy for you.**

The MFA vendor you select should provide wide coverage for a variety of applications, with plugins and easy integration. They should work closely with an identity management system. And they should provide the support that makes it easy for your end users, such as single sign-on.

As security threats continue to rise with online authentication, your organization must rise to the challenge—or face the consequences.

Learn what you need to do by visiting **www.netiq.com**.

Worldwide Headquarters
1233 West Loop South, Suite 810
Houston, Texas 77027 USA
Worldwide: +1 713.548.1700
U.S. / Canada Toll Free: 888.323.6768
info@netiq.com
www.netiq.com
http://community.netiq.com

For a complete list of our offices in North America, Europe, the Middle East, Africa, Asia-Pacific and Latin America, please visit **www.netiq.com/contacts.**

Follow us: