White Paper

Advanced Authentication

Matching Your Authentication to the Speed of Your Business

For most well-run organizations, the conflict between enabling the business to be as efficient as possible versus keeping its information and services secure is a constant balancing act or even a friction point. In today's business environment where professionals are often remote or on the go, empowering them with the tools and access they need is IT's most daunting challenge but also its biggest opportunity to deliver value.

As many businesses have discovered, there is no one-size-fits-all answer to the question of information accessibility. Because the particulars of each organization's policies and processes are unique, the criteria for vetting what the policies should be is also unique.

NetIQ

The right level of risk management is not a policy that attempts to avoid all breach hazards at whatever costs, but rather one that involves making informed choices regarding the risks the company is willing to take on as they pursue their business objectives.

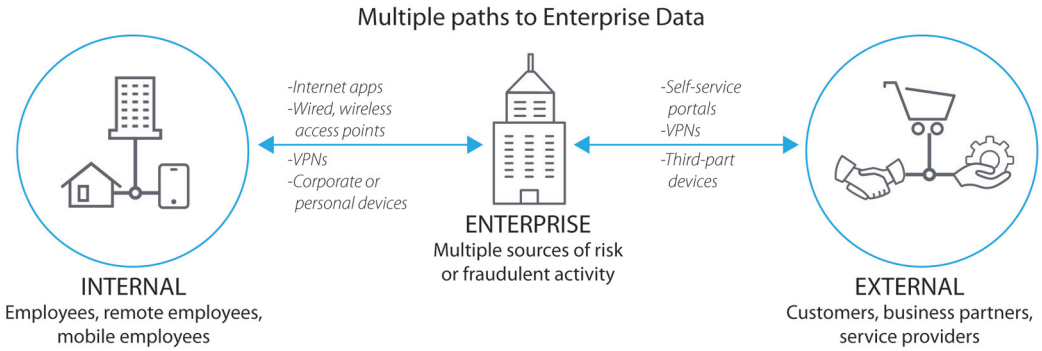
Balancing Business Risk Versus Opportunity

When it comes to deciding how much access security your organization should have in place, there is no shortcut for defining the level of risk various information types pose: private customer profiles, financial records, intellectual property, other sensitive internal information, etc. The right level of risk management is not a policy that attempts to avoid all breach hazards at whatever costs, but rather one that involves making informed choices regarding the risks the company is willing to take on as they pursue their business objectives. For example, how tolerant is your customer base if their private information is compromised? Will they still do business with you? How much would headlines of breached customer, financial, or internal information limit your ability to attract new customers?

While each organization is free to choose the level of exposure they are willing to accept, there is a more direct type of risk management for those that work in regulated industries—financial, healthcare, government, retail, etc. Government mandates. Each year, regulators set more concrete security requirements and then audit for them more aggressively. The security policy that was a suggestion last year is often a mandate within the next several years.

Whether your primary business drivers are risk, compliance, or both, the reality is that professionals are maniacally focused on doing their jobs as streamlined as possible. Each roadblock placed in their way not only inhibits their efficiency but also invites social engineering around any perceived obstacles or security annoyances. Taking this discussion to an outward facing view, how do you balance security and convenience in the way you engage with customers, clients, and patients? What level of security causes you to lose too much business?

The Reality of Today's IT Environment



NetIQ offers products that allow organizations to zero in on the important and relevant criteria and use that to deliver the user authentication and access experience that fits the particular situation.

NetIQ offers products that allow organizations to zero in on the important and relevant criteria and use that to deliver the user authentication and access experience that fits a particular situation. Security experts have noted that authentication strength is measured by its ability to resist situations where the attacker is able to falsely validate a claimed digital identity and, thus log in as that person. So, the strength of an organization's authentication environment is measured by its ability to verify a user's true identity.

Phishing continues to be one of your greatest breach threats, with user credentials being the number one target. Criminals also steal credentials from a variety of cloud-based and consumer services, knowing that people tend to use a common set of credentials across their personal and work-related services.

Authentication Considerations

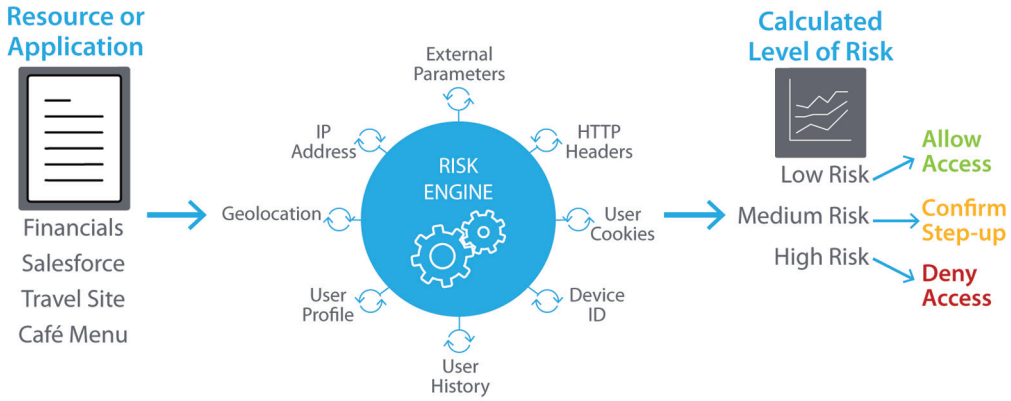
By default, there is likely a high percentage of security teams that aspire to create the ultimate identity verification system. However, today user convenience is more than your friend, it's essential to keeping the doors open and lights on. Top reasons that user convenience is a must-have requirement include:

- If there is any way possible, busy professionals aren't going to be bothered with time-consuming authentication roadblocks. To avoid credential streamlining and social engineering that increases the risk of fraudulent authentication, access should be as frictionless as possible.

Customers expect you to take precious care of their private information, but that doesn't mean that when they're on-the-road that they will tolerate a cumbersome authentication or application experience, especially if your competitor is easier to do business with.

- Customers expect you to take precious care of their private information, but that doesn't mean that when they're on-the-road that they will tolerate a cumbersome authentication or application experience, especially if your competitor is easier to do business with.
- Road warriors, field workers, as well as other types of remote professionals need a simple, reliable authentication experience. Business processes tied to time-consuming authentication will often be delayed or deferred; rather, it needs to be quick and seamless.

Risk Based Authentication



Levels of Assurance

Realizing that most organizations have authentication vulnerabilities that merit proactive measures, the National Institute of Standards and Technology offers some guidelines that business leaders should evaluate as they define the right levels of assurance for their organization.

The simplest level of assurance is where there is no identity proofing. Username and password, or some other type of cryptographic key, verifies the user's identity. Although plain text passwords or secrets are not allowed to be transmitted across a network, no other technology is used to prevent eavesdropping.

The next level of authentication requires a higher degree of identity proofing during the registration process. Single-factor remote network authentication is allowed, but it requires the claimant to prove that they control the token. If passwords are used, they must be strong, and the system must prevent eavesdropping, replay, and online guessing attacks.

The third level of assurance builds on the previous protections, but also requires the use of a soft or hard token, as well as at least a two-factor authentication. Authentication requires that the user controls the token through a password or biometric. NetIQ® Advanced Authentication provides a myriad of options that make this straightforward and simple to implement. This solution is commonly used for multi-factor remote network authentication. It not only fulfills compliance requirements for organizations that work in regulated industries but if done properly, it also provides a smooth and direct experience for the user.

NIST does define a higher level of assurance, but it is mainly for specialized use cases.

The key to designing and deploying your authentication solution is to understand your organization's exposure and match it to the right level of assurance. The art of creating such a solution is to correctly balance your acceptable level of risk against the value gained from providing a frictionless experience for your users (employees, partners, customers, citizens, etc.). NetIQ helps organizations strike this balance with a:

- Solution that provides support for a broad set of applications and services. Through Advanced Authentication's rich, built-in integrations, as well its tight integration with Access Manager and Secure Login, NetIQ can cover whatever your needs are.
- Rich identity, access and authentication heritage with expert field teams to provide information and guidance. Although organizations often believe they are in a unique situation, there is little that our teams haven't already seen.
- Standards-based approach that supports almost any authentication method and device, providing integration to existing configurations as well as future-proofing your investment as new technologies become available.

The key to designing and deploying your authentication solution is to understand your organization's exposure and match it to the right level of assurance.

Commonly, there is a rationing of competing priorities between the business owners dispersed across the organization that those of Central IT and Security who are responsible for the digital services and security.

Striking the Right Balance

Commonly, there is a rationing of competing priorities between the business owners dispersed across the organization that those of Central IT and Security who are responsible for the digital services and security.

The Security Team

Security officers are typically occupied with the responsibility of fixing firewalls, patching vulnerabilities and staying current with ever-evolving regulatory mandates. It's a constant challenge because these security teams are tasked with delivering something that doesn't guarantee 100% assurance. All it takes is one missed vulnerability or one insider breach to get a black eye. But while security officers take pains to keep current on their technical knowledge and security understanding, they are also expected to line up with the business's priorities. And as security teams work to juggle these priorities and obligations, they must also work within a budget and timeline.

The Business Owner

In contrast, business owners are focused on how to increase their revenues and broaden their market reach. In today's world, that means companies need to personalize their customer's experience as well as collaborate in deeper ways with their partners. As executives and managers reach out to their clients, they do so with targeted services and information. Business owners know if their digital customers face interaction roadblocks their attempt to engage with them will fall flat, or may even go someplace else. And yet, we all know that what looks simple on the whiteboard often turns complicated.

Additionally, business owners also know that their partners are always looking for organizations that are easy to do business with.

The Security Complexity Multiplier

If you're like your competitors, you have aggressive mobile initiatives under way. This new phase in mobility means that today your mobile app team is building applications that face the same security complexities as the web app teams of yesteryear but with the added requirement of anytime, anyplace.

In fact, today's mobile app teams face additional challenges, such as accessing external cloud-based systems that aren't integrated with existing identity and access management systems. Whatever the configuration, the same common challenges of keeping credentials and access to private or regulated information secure. Mobility is the security complexity multiplier in the art of balancing the forces of security and convenience.

While enterprises know that mobility presents an unprecedented opportunity to transform their business, the best way to get there is often elusive, resulting in disjointed pockets of tactical mobile development. The consequence of this project chaos is more impactful than an inconsistent look and feel across the corporation's mix of applications. This piecemeal approach to authentication to backend systems introduces inconsistent and uneven security. Extending user access to mobile users already increases the organization's exposure to unauthorized use and stolen devices, and abandoning a proven identity and access infrastructure broadens that exposure further.

NetIQ Access Management products enable you to navigate these new access challenges. If you want to maximize user convenience and security, you'll need to move beyond static authentication.

The Common Ground

As they navigate the balance of security verses too limiting, executives read about their industry peers who are forced to deal with the fallout of breaches or failed audits. And since both IT and the business owners want to maximize corporate value, they have a lot in common. The challenge is making it happen.

NetIQ Access Management products enable you to navigate these new access challenges. If you want to maximize user convenience and security, you'll need to move beyond static authentication. Static authentication ignores the situation or context of the request. An internal user accessing private information from the office during work hours doesn't present the same level of risk as does a remote user. To complicate matters, gone are the days when employees work nine to five or even within the walls of the office where access is delivered in a predictable, simple and easy-to-secure fashion. Today, employees expect to work from anywhere, using the device of their choice.

Today external users (customers, partners) will be using a myriad of devices from all sorts of locations. Remembering that it's quite possible that these users can have their credentials stolen or hacked, you will need to gather evidence of their request for access and use it as a metric for calculating the risk. Common metrics that can be used to verify a person's identity include:

For situations where step-up authentication is warranted, having an authentication solution that supports the widest range of authentication methods makes it complete. NetIQ's Advanced Authentication gives you just that.

- What level of risk does the location denote: "Office or home? Recurring or new? Local or remote?" NetIQ has some unique technologies here, making it easier and more effective to implement than ever.
- Is the user at two places at the same time?
- Has the device been used previously and has it been tied to a verified user?
- What level of risk does the artifact or service pose to the organization: general information or private and sensitive?

Your organization might be the type to defer or procrastinate the use of dynamic authentication. Here's a reminder of how to get your projects off the ground and keep them going.

- Start small and target early wins. Risk-based authentication can get complicated quickly. Requiring hefty investments (time and money) often results in inaction. Instead, target assets that need the most protection for sensitivity and frequency of remote access. Also target risk assessing metrics that are simple to gather and that deliver worthwhile gains over traditional credentials.
- If you are a security officer, make sure the business stakeholders know that dynamic authentication is all about making access to everything quick, limiting step-up authentication to the resources that need it.
- Balancing the speed of access with security will be a continuing, iterative process. Incorporate the easiest metrics first and evolve from there. You want to target the biggest risk areas and manage them with the easiest risk assessments.

Beyond Dynamic Authentication

Of course, adapting the authentication type is only part of the equation. For situations where step-up authentication is warranted, having a solution that supports the widest range of methods makes it complete. NetIQ's Advanced Authentication gives you just that. While you might want to allow most of your users to use two-factor authentication with their smartphones, organizations who need to take into account higher risk situations may choose to use a specialized token or biometric authentication option. NetIQ allows you to accomplish all of this with a single framework and one set of policies, keeping overhead to a minimum and authentication consistent.

Worldwide Headquarters
515 Post Oak Blvd., Suite 1200
Houston, Texas 77027 USA
+1 713 548 1700
888 323 6768
info@netiq.com
www.netiq.com
www.netiq.com/communities/

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

www.netiq.com