WHITE PAPER

Today's Risks Require Tomorrow's Authentication

As businesses, other types of organizations, and their customers increasingly interact and transact through their laptops and mobile devices, the need to protect their resources and information dramatically increases. Both the number and the seriousness of breaches continue to rise at a steady pace, most of which involve compromised or vulnerable authentication. This white paper discusses the changing landscape and business drivers behind the need for multi-factor solutions.

NetIQ | WHITE PAPER

Table of Contents

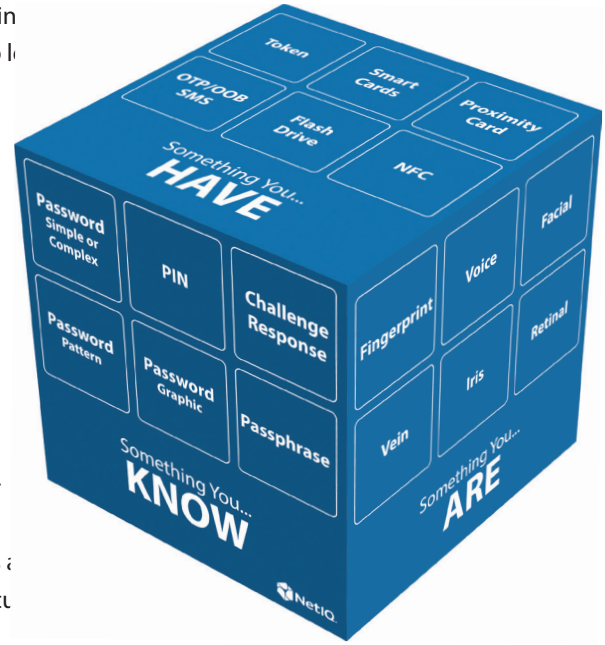
Responding to Today's Security Threats

The transformation of how people work and play continues to evolve towards a mobile lifestyle where people don't need to be in the office to work or at the store to shop. In fact, according to IDC , 1.3 billion of today's workforce is mobile. In other words, one third of today's workforce works outside of the office.

For many professionals, the ability to stay connected using phones and the Internet enables them to accomplish tasks, collaborate with colleagues and specialized teams, and conduct most types of business interactions. However, these same trends create points of vulnerability for unseen criminals. The internet provides the connectivity and interconnected social media platforms that result in an expansive attack surface for criminals to circumvent traditional authentication and access protections .

As the continual stream of headlines shows, this new paradigm of engaging with applications and services beyond the corporate firewall changes the rules for how organizations manage risk and apply security. The ramifications of breaches are real and sometimes very damaging. In addition to the immediate financial cost that breaches incur, frequently customer trust is lost, brand reputation is tarnished, and, in instances where regulated industries are involved, privacy rules are violated, creating additional costs and potential fines.

NetIQ believes traditional, single-factor authentication, including username and password, is no longer a sufficient approach to protecting corporate, employee or client information. And as a result of the increasingly sophisticated attacks being levied at users and organizations, the paradigm of protecting against unauthorized access must also evolve. Users and their devices are continuously connected and exposed to a variety of attacks. Even when users are working from inside an organization's facilities, many of the services they access no longer reside inside their firewall's perimeter, but rather out in the cloud, allowing ubiquitous access for all, both friend and foe. Moreover, since criminals and conspirators have gotten quite good at duping people into divulgin credentials (what they know), an effective way to increase security is to l what they have (such as a FIDO U2F device) or what they are (such as a biometric reader). The use of these various authentication methods is called multi-factor authentication (MFA).



If done right, combining two or more authentication methods makes it exponentially more difficult for the bad guys to circumvent access policies, reducing the risk to the organization. This paper discusses the changing trends of how professionals inadvertently create risk to the organization as they do their jobs and blend their professional and personal lives by consuming and sharing information. It is intended for individuals who are researching and gathering information in preparation of a proposal or business case for enhancing an organization's authentication. This information provides a foundation from which an organization can move beyond passwords a upgrade the authentication experience to a level that increases the secu maintaining or improving user convenience.

[1] http://www.eweek.com/c/a/Mobile-and-Wireless/Mobile-Worker-Population-to-Reach-13-Billion-by-2015-IDC-238980

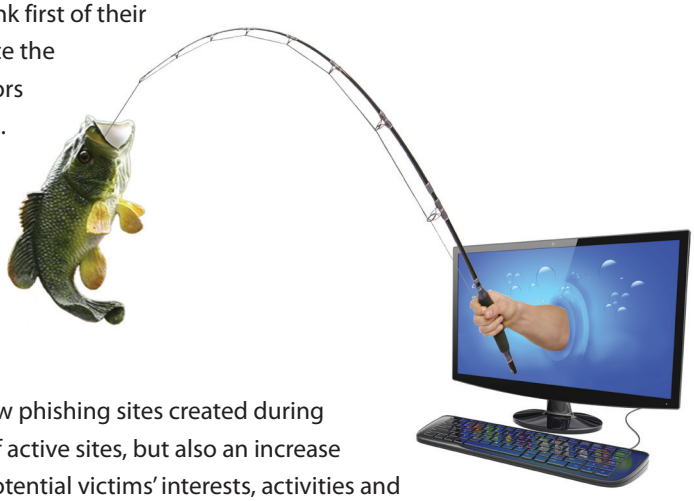
[2] http://blog.trendmicro.com/most-data-security-threats-are-internal-forrester-says/

Today's Breach Trend is Clear

The job of managing against risks associated with the use of traditional credentials continues to elude IT administrators. In fact, it is more difficult than ever before because users connect to both personal and corporate services with the same device, which is often personal. If given the opportunity, many users would simplify life for themselves by using weak passwords or writing them down. And even if policies exist to protect against users who would otherwise rely on simple passwords, security can still be susceptible to social engineering, intentional or otherwise. Users that blend their personal (and often less secure) credentials with those used to protect private corporate or customer information introduce one of today's most challenging risks. This expands the attack surface where if one instance of the user's credentials is compromised, it also risks exposing corporate services. Unfortunately, as seen frequently in the press, months usually go by before victimized institutions realize the breach and alert the public. Regardless of the password policy implemented, if a user reuses a password across his or her professional and personal (social) services, the risk of a breach escalates. Each security team needs to have a plan in place that manages the vulnerability of reused credentials across multiple cloud-based systems.

For environments where employees move from station to station or room to room, the pressure to share credentials increases. Credential sharing can be convenient and highly efficient and is especially prevalent in industries such as manufacturing, defense contracting and healthcare. These shortcuts may save users time, but this is at the expense of security. While healthcare clinicians often fall into this practice in environments where they move from patient to patient and are pressed to optimize their time, this type of situation can be found throughout many organizations—from call centers, banks and retailers, where customer information may be at risk, to government agencies and their contractors where all types of secured information are at risk.

Although unseen criminals continue to raise the level of sophistication in their attacks, a report jointly issued by Forrester and Trend Micro notes that threats more frequently come from someone inside the organization. In fact, 70 percent of the time, unauthorized access comes from someone within the organization, or a contractor working within the secure perimeter . Although IT organizations may think first of their employees, several high-profile intrusions highlight and reinforce the problem of contractors sharing their credentials. Since contractors are often in transition, this tends to be a more frequent problem. It's not unheard of for contractors to focus on their specific project with the here-and-now attitude at the expense of the security of an employer or customer with whom they don't have a long term relationship. But whether it's an employee, contractor or partner, the workforce's ability to share accounts is shortsighted and subjects the company to undue risk.



In their recent threat report, McAfee Labs describes a million new phishing sites created during this past year. The report highlights not only the rapid growth of active sites, but also an increase in their sophistication . Widely available digital content about potential victims' interests, activities and where they work makes it easier for phishermen to learn about and more effectively attack their targets. Whether it is

[3] http://blog.trendmicro.com/most-data-security-threats-are-internal-forrester-says/

[4] http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2014.pdf

[5] http://media.ofcom.org.uk/news/2013/uk-adults-taking-online-password-security-risks/

an email claiming to be from a friend, organization, work, or some other party with whom that person interacts, these emails and websites look authentic enough for unfortunate users to make that click that enables a keylogger to be downloaded or invites them to divulge their credentials.

User education against phishing is the single most effective step an organization can take against these kinds of attacks. Antivirus and malware protection are the basic steps that every organization should take, but upgrading to an MFA for valued information is equally important and should be included in the majority of organizations' defense plans. Advanced authentication technologies can be used for out-of-band identity validation to protect compromised accounts and man-in-the-middle vulnerabilities. When implemented correctly, it will significantly increase security for virtually all environments.

In today's universally connected digital world, how much risk should an organization be willing to take? Whether it be through users implementing common credentials across their work and home environments or account sharing, betting on a single point of credential protection failure is becoming more foolish as attack mechanisms continue to increase in sophistication. Even for organizations that have strict password complexity policies, their value is limited when they are reused repeatedly on other websites. Recent studies show that more than half (55%) of adult internet users admitted that they use the same password for most, if not all, of their websites . As the consumption of cloud-based applications continues to proliferate, the chance of compromised credentials draws nearer to inevitable.

Working within Regulated Industries

While each organization is free to choose the level of risk they are willing to take, they don't have the prerogative to choose which regulations they will follow. Each year, regulators set more specific security requirements and audit more aggressively. And as the number of access breaches continues to rise, this trend is likely to continue.

Healthcare

Regulators significantly changed the Health Insurance Portability and Accountability Act (HIPAA) in the last several years. Privacy rules continue to become more encompassing and detailed. There is a greater liability for those who fail to implement technologies enabling compliance to HIPAA and Health Information Technology for Economic and Clinical Health (HITECH) rules. For example, specific consequences and accountability for violations and breaches are now in place. And if unauthorized access of regulated patient records occurs, organizations must notify the department of Health and Human Services and their patients of the breach. If the breach was the result of the organization not following HIPAA or HITECH rules, regulators now require a detailed plan of how the organization will become compliant, as well as the timeline for doing so.

As organizations strive to meet compliance, the Office for Civil Rights (OCR) continues to find ways to be more effective in their auditing programs. To accomplish this, they work with auditing firms as well as the healthcare agencies themselves to implement a combination of self-auditing and health checks.

Financial

Federal agencies responsible for the compliance of financial and insurance institutions established rules, guidelines and audit procedures to ensure regulated organizations aggressively manage risk. A high level of security is a foundational component for making transactions as secure as possible. The Federal Financial Institution Examination Council (FFIEC) published rules for implementing proper authentication

methodologies to match the level of risk involved in the transaction. FFIEC instructs IT organizations to take a risk-based layer of security approach in their implementation and have the ability to perform reviews of an institution. Because of these strict rules surrounding access, advanced authentication is a fundamental requirement to whatever access environment a financial institution offers.

Federal

IT security managers in federal agencies face increasingly complex challenges as they try to keep up with their access control requirement. These agencies commonly have unintegrated silos of authentication environments, each requiring their own point of administration. In addition, most of these deployments locked the federal agencies into specific brands and types of authentication solutions. The National Institute of Standards and Technology (NIST) issued additional publications providing concrete guidance for these Federal Information Security Management Act (FISMA) mandates. They provide guidance on access controls and permission management, both of which should be based on strong authentication. In other words, performing certain actions or accessing specific information requires some type of advanced authentication method.

State and Local Organizations

Virtually all state and local agencies rely on federal databases for information on people of interest. To gain access to these databases and records, agencies must comply with government access and authentication requirements. The Criminal Justice Information Services (CJIS) defines and enforces policies to ensure that their information (CJI) remains secure and protected from unauthorized access. These policies include requirements for the creation, viewing, modification, transmission, dissemination, storage and destruction of CJI data. A fairly recent change in this policy is the requirement for the use of advanced authentication methods when accessing this information outside of a federally approved (secure) building. As a result, this mandate affects all personnel accessing CJI from their homes or squad cars.

The latest mandate has the potential to make CJI access quite difficult for state and city agencies. They often have one or more building-access infrastructures in place, but they are seldom integrated and require multiple touch administration. For many agencies, this mandate will result in yet another authentication solution and additional point of administration. However, NetIQ® Advanced Authentication Framework handles most authentication methods and provides a single set of policies and point of administration. NetIQ Advanced Authentication Framework not only ensures authentication compliance, but also equips organizations with what they need to adopt different or newer authentication technology in the future, without deploying another instance of infrastructure.

The Evolution of Secure Access

While security is and should be the fundamental requirement when deciding on an authentication solution, convenience is just as important. In fact, the ultimate measure of success of an authentication process is how effectively the business keeps its information secure while preserving the ease of accessibility over time. If users abstain or procrastinate completing tasks or business processes because authentication and access

is cumbersome, the solution in place falls short. If employees avoid using business services or look for ways to get around them using their own tools because the authentication and access experience is complicated, productivity and security take a notable hit. Furthermore, if the selected advanced authentication solution is time consuming or complicated to enroll, the cost of deployment and training will likely keep the authentication project from being implemented.

As if the problem of delivering secure access isn't complicated enough, the standards for making mobile access convenient have recently been raised. What was an acceptable level of convenience five years ago is inconvenient today. This makes delivering secure, convenient access that protects against attacks and threats from a highly connected world a great challenge. The same technology that connects people to services and defines what is convenient and usable is also the technology used by attackers. So when organizations think about MFA usability requirements, they need to consider more than just employees—they also need to take into account customers, contractors and partners. This is important because for many organizations, the solution that offers the widest authentication methods, the broadest application-authentication solutions, and the lowest total cost of ownership is often going to be the best option.

Mobile phones and tablets have also evolved personal interaction. People are more connected and conduct more business at anytime from anywhere than ever before. As such, mobile technology has become an essential component of the way that professional and business communications and interactions occur.

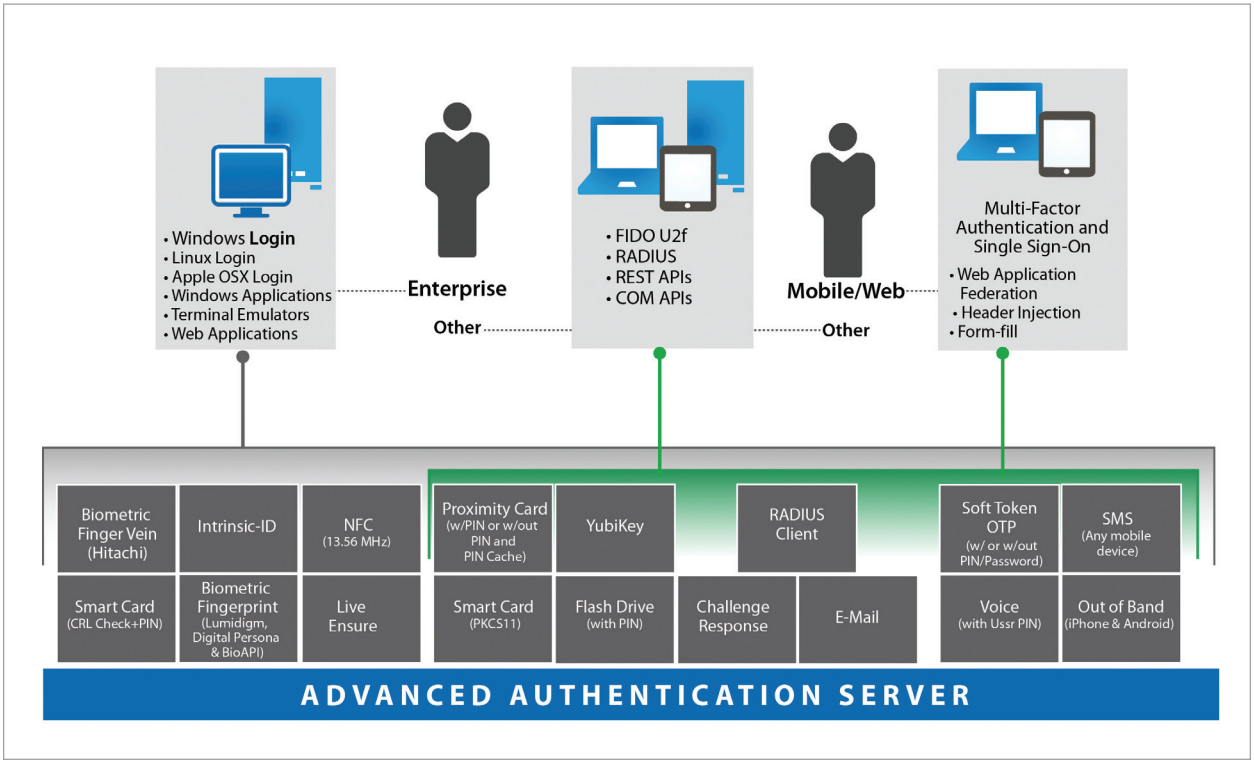
Enterprises now recognize that their customers expect to interact and make transactions with them on mobile devices. Customers also expect enterprises to continue to introduce new ways to be more accessible. Organizations need to personalize the mobile experience while allowing customers to access an unprecedented level of private information that must be secured. But there is more at stake than the customer's security. What if the customer experience pales in comparison to the competition, offering less functionality or providing a cumbersome mobile access experience? Complicated authentication and access experience damage the corporate brand, reduce consumer loyalty and limit customer engagement. MFA has become more than just security; it has become the face of the business to the customer. This means organizations need to plan on adding or updating their MFA to include the latest technologies to keep the customer experience fresh. If this isn't planned, organizations will experience multiple authentication frameworks or service providers that raise the costs of solutions, add to administration hours and create situations where inconsistent policies open the way for a breach.

It's surprising how often the roughest patch of an MFA deployment is user enrollment. If enrollment requires the user (customer, employee, contractor, partner and so on) to go through a number of steps or installations, the rollout will fail. In addition, cost of enrollment needs to be a primary consideration when researching types of authentication methods. And, as stated earlier, high on the list of considerations is preparing for the future and what it may potentially offer.

Moving Forward

Today's breach trend will not abate for the foreseeable future. At the same time, IT's control over organizations' vulnerabilities decreased over the years and will continue to do so. The number of cybercriminals has exploded, and they have more weapons that are far more sophisticated than ever before. As services continue to move to the cloud, a smaller percentage of them remains inside the corporate firewall. More people embrace bring-your-own-device (BYOD) or work outside of the office. This means that people constantly connect to and interact with various social and commerce services on the internet, which broadens their attack surface exponentially.

Essentially, BYOD and mobility trends cause traditional usernames and passwords to become progressively ineffective as cybercriminals continue to exploit them, as well as other types of single-factor authentication methods. Risk to the organization continues to rise without a reinforcement of the authentication process that confirms the user's identity.



NetIQ Advanced Authentication Framework – for today and tomorrow

As you look for solutions that give you choice and flexibility for both current and future MFA needs, NetIQ ensures that you won't get locked into authentication silos or stuck with outdated technology. NetIQ offers an open framework that aggressively updates as new technologies emerge, including compatibility with FIDO U2F-based devices.

In addition to the MFA flexibility that NetIQ Advanced Authentication Framework offers, it also comes out-of-the-box integrated with the market leading single sign-on solution from NetIQ, which covers virtually all applications and most platforms: NetIQ® Access Manager™, NetIQ® CloudAccess and NetIQ® SecureLogin. Having a robust single sign-on solution is an essential element of convenient access by delivering access to all the user's relevant services. For ubiquitous compatibility, NetIQ Advanced Authentication Framework also integrates with other single sign-on solutions.

To learn more about NetIQ Advanced Authentication Framework, or to start a trial, go to www.netiq.com/AdvancedAuthentication.

About NetIQ

NetIQ is a global, IT enterprise software company with relentless focus on customer success. Customers and partners choose NetIQ to cost-effectively tackle information protection challenges and manage the complexity of dynamic, highly-distributed business applications.

Our portfolio includes scalable, automated solutions for Identity, Security and Governance and IT Operations Management that help organizations securely deliver, measure, and manage computing services across physical, virtual, and cloud computing environments. These solutions and our practical, customer-focused approach to solving persistent IT challenges ensure organizations are able to reduce cost, complexity and risk.

Learn more about our award-winning software solutions at www.netiq.com.

562-001019-001 DS 07/15

Worldwide Headquarters
515 Post Oak Blvd., Suite 1200
Houston, Texas 77027 USA
Worldwide: +713.548.1700
U.S. / Canada Toll Free: 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**.