BYOD and Cloud Have Changed Everything

If you’re like most businesses, you’re probably dealing with BYOD and remote users needing access to data and applications—their work “stuff.” As personal smartphones and tablets have become ubiquitous, BYOD has increasingly become part of the mainstream IT world. That’s because keeping workers productive is a priority for many businesses.

This emphasis on productivity is nothing new. For years, businesses have implemented ways of making it possible for employees to work from remote locations. But providing access is not as simple as it once was. Access used to be fairly straightforward because IT was able to control it all. You could provide access via VPN from beyond the firewall—and that connection was usually made using a company-provided device. Further, the applications and data being accessed were almost universally on-premises. This gave IT a great deal of control over the entire environment.

Today’s environments are trickier to manage than ever before. First, users want access from their own device—not a device controlled by corporate IT. And the applications, data and services they’re accessing aren’t all in the corporate data center. Increasingly, organizations have a mix of on-premises and in-the-cloud solutions. This combination of devices and services that IT doesn’t control can make managing access and maintaining productivity a real challenge.

But simply providing access isn’t enough. Users will tell you that they just want access, but that isn’t strictly true. They want access, and they want the system to perform well and be easy to use. Plus it isn’t enough to provide access to some systems but not others. Users want (and need) access to everything in order to stay productive. Finally, there’s the question of security. Access is relatively simple. Secure access—a necessity in today’s corporate environments—is much more difficult. Solving for both productivity and security is an increasing challenge in today’s complex technology world.

Take Stock of Your Environment:

1. What are your current investments?
   - Infrastructure
   - Access controls and processes

2. What will you need to support in the future?
   - Legacy applications
   - Cloud solutions

3. What does your employee or user behavior require?
   - Devices
   - Locations
   - Mobility
Access Should Start with Your Environment

Fortunately, there are many options for addressing today’s mobile and BYOD challenges. In fact, as more and more services are moving to the cloud, there are an increasing number of cloud-based solutions that manage access. This is a popular option, and one that several vendors and some analysts are emphasizing right now. But on-premises options exist as well—so how do you decide which is best for you? It may seem obvious, but the first step is pretty basic: Take stock of your current environment.

The first thing to consider is your current investments. Most companies have made large financial investments in systems and infrastructure that cannot be ignored. To support that capital expenditure, there has been the operational expenditure of developing core competencies and skills within your in-house team. Beyond the CAPEX and OPEX investments, most businesses have invested considerable thought in developing both the access infrastructure and the logic or business rules that support that infrastructure.

The second consideration is your IT environment moving forward. What legacy systems will your business require? Which applications are you likely to add? What access controls and processes are currently in place and how complex are they? Most companies are supporting a mix of on-premises and cloud-based solutions. But it is often difficult to say with certainty which ones can (or even should) move to the cloud in the future.

Finally, consider the needs of your users. What applications do they use most often? What are their expectations for your organization? How mobile are they? And perhaps most importantly, what devices do they expect to be able to use? Consumer technology now outpaces business technology in terms of user experience and functionality. This trend will continue to drive user expectations and increase the importance of delivering not just basic functionality, but a good experience as well.

With so many applications moving to the cloud, it would be easy to focus your BYOD initiatives there as well. But as you look to solve today’s access and security challenges, don’t neglect internal applications, processes and resources. They represent a substantial corporate investment and are often just as critical to maintaining user productivity as cloud applications are in today’s BYOD world.

Choosing the Right Solution

There are quite a few solutions out there, and picking the right one can be a real challenge. However, there are some things that you should consider. As you evaluate your choices, make sure that you choose an option that will:

- Maximize your confidence in security.
  With many cloud-based services, you never hear about security breaches until after they happen. If your cloud-based access provider is subject to a hack or intrusion, how quickly will you know that you’re at risk? And how quickly will you be able to respond if your data is exposed?
- **NetIQ® SecureLogin.** Streamline user authentication for enterprise applications by providing a single login experience to users through multiple login methods.

- **Ensure your ability to meet internal SLAs.** While most cloud service providers have some kind of performance guarantee, you have to ask yourself who is ultimately in charge of the performance of the tools? More importantly, who is going to be held accountable if those SLAs aren’t met?

- **Cover all of your applications.** Once again, consider your environment. Will the cloud-based solution accommodate your desktop apps as well as cloud- and browser-based apps? Can it accommodate native phone apps? How about legacy systems? Consider all of your applications and services before deciding.

- **Be affordable for the long term.** Cloud-based services are attractive because they typically have a low cost of entry. But you have to think beyond the purchase price. Consider per-user, per-month expenses that continue over time. While acquisition and implementation costs may be low, the accumulated ongoing cost of subscription-based services can quickly surpass the cost of purchasing a solution outright. Also, consider the additional management time that your team will spend.

- **Provide organizational value beyond simple access.** As you evaluate options, consider how an access solution can work with future plans and other systems. Will the solution support the type of advanced authentication you need if and when you decide to implement it? Will it integrate with your existing security policies? Will it be easy enough for users and administrators to deliver the benefits you expect? Can it support productivity enhancements such as single sign-on across your technology environments?

  Consider your needs and options carefully when selecting a secure access solution for your BYOD needs. Just because a solution is the “hot” alternative, doesn’t mean that it is going to be the best fit for your organization. A considered approach will help you decide what makes the most sense for you.

NetIQ has a range of options that can help address your BYOD needs. Our Identity-Powered Solutions use identity information intelligently to make your business more responsive and secure. They leverage your existing resources and infrastructure so you don’t have to start from scratch. And they deliver sustained business value while driving lower TCO. Specific products that can help with BYOD include:

- **NetIQ Access Manager™.** Deliver simple, secure, scalable web access to internal and external resources, with standards-based federation and support for advanced authentication.

- **NetIQ CloudAccess.** Provide simple access to your private or regulated information hosted in the cloud. With NetIQ CloudAccess, you can offer secure mobile access for BYOD users with simplified single sign-on access that spans environments.

**About NetIQ**

We are a global enterprise software company that meets the demands of today’s IT environments with a wide range of proven solutions for identity and access management, security and data center management.

Today’s hybrid IT infrastructures are creating new challenges for business and IT leaders. IT services are now being delivered across an increasingly fragmented combination of physical, virtual and cloud environments. These services are being accessed from an expanding number of locations, on a growing variety of devices. And the technology environment is changing faster than ever. In the face of this combination of forces, organizations like yours often struggle to balance consumerized user expectations with the need to reduce organizational risk. All
while still embracing the business value that can be achieved by leveraging innovations like cloud computing, cloud page, and mobile technologies.

So how do you keep access to IT services simple, while preventing unauthorized or risky user activity—all in the context of where and how users are connecting? That’s where NetIQ comes in. Our broad portfolio of solutions helps you manage the complexity of hybrid environments to ensure that the right people have the right level of access to the IT services they need, whenever they need them. With NetIQ, you can incorporate new technologies and services more securely, faster and with less effort. And our solutions help you understand what is going on in your environment—in real time—so you can mitigate risk while still taking advantage of opportunities.

Quite simply, this means that you can secure, manage and measure what matters most to your organization. Even more important, this new level of clarity will create new opportunities—and competitive advantage—by enabling you to understand, maintain and make sense of the shifting relationships between individuals, devices, behaviors and technology services. That’s how you can drive the successful business outcomes that will deliver ongoing value to your organization.

Learn what next steps you can take by visiting: www.netiq.com/solutions/identity-access-management/secure-mobile-access.html