Managing the Consumerization of IT: Mobile Access for the BYOD World

The Consumerization Conundrum
Welcome to the new world of technology, where personal devices deliver a superior experience to business systems. It’s no coincidence that a recent Microsoft survey suggests personal technology has a significant and positive impact in transforming our lives as well as innovation in business. As consumers, we are increasingly attached to our personal electronics, even to the point of sleeping with our devices.

It should come as no surprise, then, that consumers are increasingly intent on using their personal devices for work. This trend spawned the term “bring your own device” (BYOD), and it has been a controversial topic for many IT organizations. Done right, BYOD can improve both productivity and job satisfaction. But done incorrectly, it can frustrate employees and lead to significant security concerns.

Although BYOD isn’t a new concept, for most companies it is still only partially resolved. According to CIO Magazine, BYOD has become the “new normal” for business, to the point that by the start of 2013, three-quarters of organizations had a BYOD program in place. But of those, two-thirds had adopted an anything-goes approach, with little governance.

The wide-open approach has done a lot to bring personal devices into the workplace, creating justified concerns about risk. In 2012, Ovum pointed out the growing risk from unmanaged BYOD. This message is reaching a wider audience on the business side as well as the IT side of the organization.

CIO MAGAZINE POINTS OUT THAT: “The [mobile device management] vendors’ message that the cost of compliance is a fraction of the cost of non-compliance was bolstered by the chilling effect of the [Edward] Snowden affair. More than a few business managers realized the consequences of poor BYOD security and the dollars at stake, and so they began reaching out to IT for help.”

According to Gartner, 20% of BYOD initiatives will fail because of management measures that are too restrictive.
The bottom line is that, despite statistics that show high levels of BYOD adoption, many businesses still haven’t completely figured out how to capitalize on BYOD without exposing themselves to risk.

To further complicate matters, BYOD is a moving target. Today’s fringe technology may be a business essential tomorrow. The iPhone, once derided as not enterprise ready, is now firmly entrenched in business. And BlackBerry, once the enterprise standard, now has a market share lower than the lowly “other” category in industry reports. The forthcoming wave of wearable devices may not seem like they have a place in business today, but that may change tomorrow. Google Glass, for example, is maligned in some news stories, while others suggest that it will be transformative. The truth is, we don’t yet know which devices will find their way onto corporate networks next. We do know, however, that more and more devices are connected, and that people are embracing new technologies at an amazing rate. And that’s the fundamental, ongoing challenge of BYOD: enabling the technology that users want and giving them access to corporate systems without increasing risk.

Current BYOD Solutions or Alternatives Don’t Really Solve the Problem

As the CIO article cited above suggests, IT departments have been charged with finding ways to embrace BYOD while maintaining compliance. Unfortunately, many of the solutions—like mobile device management and a corporate-owned device policy—come with drawbacks.

Mobile device management (MDM) seems like an obvious choice for corporate-owned devices. You simply install an application (or “agent”) on a device that allows you to wipe data in the event the device is lost or stolen. But MDM can be a challenge when users bring their own device:

1. **Do users really want to give IT the ability to wipe their devices?**

2. **Even with containerization, employees are still giving up some control over their device. That idea is especially unappealing to many users since BYOD is by definition a personal device.**

3. **Many employees are concerned about losing their privacy, or installing anything that enables their employer to track them.**

4. **Many employees are hesitant to allow their employer to take control of even parts of their personal device.**

5. **Gartner points out that 20% of BYOD initiatives will fail because of management measures that are too restrictive.**

The MDM market is growing, but data shows that deal sizes remain small. That suggests most businesses are only actively managing a small subset of devices within their environment. So while MDM does resolve some BYOD concerns, it perpetuates many of the end-user objections that brought BYOD about in the first place.

An alternative to BYOD is COPE (corporate owned, personally enabled). It attempts to bypass the need for BYOD by reversing the model. Instead of employees using their own devices for corporate access, it provides corporate-owned devices that can be used for personal activities as well. COPE inherently involves MDM—but is less objectionable because the company owns the device. But COPE doesn’t address the ongoing desire of users to choose what they want and upgrade when they want. Nor does it address the concern that a corporate Big Brother might be watching the device, snooping on the user and the data.

A mobile application access solution allows you to capture the advantages of BYOD while minimizing the risks.
Both MDM and COPE share a fundamental flaw that is rooted in the very idea of BYOD. They focus on the most disposable, least secure, most easily stolen or otherwise compromised part of the equation: the device.

Focusing on applications has several advantages. Moving the credentialing process off of the device can increase security. It makes it easier to expand access to cloud services. It lets you put everything users need in one place—a portal to all critical business apps. It can even allow for single sign-on, reducing how often users need to re-authenticate. It allows administrators to define and manage access easily. And finally, it allows organizations to take advantage of the cost savings of allowing users to purchase the devices they want. In short, a mobile application access solution allows you to capture the advantages of BYOD while minimizing the risks.

**Things to Look For in an Access Solution**

As you evaluate solutions, consider what your organization really needs. Ensure that any option you choose:

1. **Allows you to extend security policies to more endpoint devices so you can increase access and productivity without increasing risk.**
2. **Is convenient and actually makes users’ lives easier (otherwise, they won’t use it).**
3. **Enables users to keep their personal devices personal.**
4. **Allows access to legacy web applications without the need for a native mobile application.**

Consumer devices will continue to evolve. Your business must find a way to take advantage of the technology employees want to use—without opening your organization up to additional risks.

Changing the way you think about BYOD is key to controlling risk and protecting your organization’s private information—from intellectual property to customer information, regulated data and more. NetIQ can help deliver access tailored to the device. To learn more, visit the NetIQ® Secure Mobile Access page: [www.netiq.com/products/cloudaccess/features/byod-secure-mobile-access.html](http://www.netiq.com/products/cloudaccess/features/byod-secure-mobile-access.html)