Embracing BYOD in the Enterprise

Executive summary

Five or ten years ago, the notion of self-service IT would be unbearable to most enterprise IT executives. Facing the challenge of supporting a fast-growing user base with fixed IT resources, IT teams made control and standardization a central focus. In the IT team’s ideal scenario, only a small number of influential users would be allowed to deviate from the standard corporate hardware and software options.

Today, the concept of “Bring Your Own Device” (BYOD) is challenging the traditional IT mindset of device-centric control. It initially began as a financial discussion, with some organizations considering whether they could move traditional corporate PCs off the company balance sheet by shifting ownership to users via financial incentives. However, it was the emergence of highly desirable user-centric computing devices like tablets, smartphones, and ultrabooks that catapulted BYOD from a conceptual topic to an unavoidable force that IT teams must deal with.

While BYOD may seem like a relatively new IT topic, Forrester Research estimates that over 53 percent of workers use their own technology for work purposes. Most alarming for IT leaders is the fact BYOD is starting in the executive suite. Forrester estimates that a staggering 77 percent of executives buy their own hardware, so ignoring BYOD is more perilous than most user-driven technology trends.

AppSense believes a shift to a people-centric computing approach is the key to mitigating the added risk and complexity introduced by BYOD. By shifting management and policy focus from devices to users, a people-centric strategy allows IT teams to prepare for a world with significantly less device standardization and control without compromising efficiency, security, or compliance.

Once user experience, data, and application access can be managed at level above the device, multiple options for supporting BYOD users emerge. For many organizations, this may begin with delivery of remote desktops and applications to untrusted devices, and there are valid use cases for this approach. However, AppSense believes that the true answer to the BYOD challenge is to enable a native experience on the user’s device of choice without compromising IT visibility and control. With either approach, avoiding device-level complexity through a people-centric approach is key.

People-centric computing and BYOD

The origins of BYOD and the myriad management challenges it raises will be outlined in the sections that follow, but a central theme that will emerge is that shifting policy and management focus to users is a strategic imperative. This is not to say that traditional needs for device-level management disappear. Rather, it must be assumed that users will need to roam between multiple devices, including some that are not trusted or controlled by IT, and management tools and strategies must be realigned accordingly.

A new reality of supporting enterprise IT services on untrusted devices means that enterprise IT teams must make existing Windows-based computing more dynamic, as well as explore new ways to enable secure data and native application usage on personally owned tablets and smartphones.
Creating context-aware desktops

Even as users shift a portion of their computing workload to non-traditional operating systems such as iOS and Android, many will continue to use Windows as their primary computing environment. However, virtualization and BYOD increase the likelihood that a user access their Windows-based desktop from several different device types.

Therefore, a best practice for IT teams is to dynamically adapt the Windows experience based on the usage context. This may include dynamic configuration of the Windows experience to, for example, optimize for touch when being accessed remotely from an iPad. It may also include security-focused measures such as limiting administrative rights when the desktop is being accessed from an unknown or untrusted device.

The ability to dynamically personalize and adapt a desktop based on context also gives IT teams an important countermeasure against loss of standardization, a related challenge that will be explored in more detail below. Reducing the complexity of what is in place frees time and resources to focus on new BYOD management challenges.

Through products such as Environment Manager and Application Manager, AppSense already gives IT teams a wide range of tools to make the core Windows desktop environment more adaptive. However, this is only part of the BYOD equation, as BYOD is increasing pressure to allow and support a wide range of non-Windows mobile devices.

Enabling seamless enterprise mobility

The ideal end point for a people-centric computing strategy is a world where users can use any corporate or personal device with a frictionless, native experience that does not compromise IT efficiency, information security, or compliance.

For many enterprises, this seems like a place on the distant horizon. However, AppSense is actively engaging with enterprises to extend beyond the Windows world to enable BYOD models that balance user satisfaction and convenience with sound IT practices.

The first step to enabling enterprise mobility with a native user experience is addressing the data access challenge. There are a growing number of products and services focused on this challenge, but AppSense is unique in its philosophy that the answer is improving access to existing infrastructure without adding a new layer of complexity or introducing new security and compliance challenges. This is the design philosophy behind AppSense DataNow, the latest addition to the AppSense product family.

AppSense's strategy, however, does not end with data access. Once enterprise data reaches an untrusted personal device, a new question immediately arises: “What will the user be allowed to do with this data?” Building on a rich history of providing granular policy controls, AppSense is focused on extending enterprise policy to data, as well as enterprise applications on untrusted devices.

Why prepare for BYOD?

The short answer: you don't have a choice. IT leaders are accustomed to setting their own priorities based on strategic objectives such as higher service quality, cost reduction, or improved security. BYOD began as one of these traditional initiatives that IT teams could chose to embrace or defer. However, new devices and evolving user preferences are forcing BYOD onto the enterprise IT agenda.

Company-sponsored BYOD programs

Mainstream discussion about BYOD programs first centered on the idea of shifting ownership of traditional Windows-based PCs from the corporation to users. The theory with this approach is that ongoing capital costs of PC hardware can be removed from the organization's balance sheet in favor of a predictable flow of stipends to the employee base. While this seems appealing on paper and is being implemented in some organizations, it remains a niche.

Given the importance of uninterrupted computing to most organizations, IT teams are generally optimized for service availability over cost. Implementing major changes to the enterprise computing infrastructure is risky, and there are many unknowns concerning possible increases in support costs due to extreme loss of standardization. Even if the BYOD program specifies certain PC models that may be used, personally owned machines come with an expectation that the user is free to customize at will.

Embracing BYOD in the Enterprise
Embracing BYOD in the Enterprise

For most organizations, the benefit of savings on a balance sheet does not tip the scales against the risk of lost employee productivity. However, as broader industry shifts lead employees themselves to push for BYOD approval, it is likely that company-sponsored programs will be more common. The aforementioned Forrester research findings indicate that within 36 months, most IT organizations will shift from a reactive stance on BYOD to some type of formal support model.

Employee-driven BYOD pressures
The most immediate BYOD pressure that IT teams face is coming from users themselves. This began with the introduction of smartphones that are useful for productivity tasks above and beyond basic e-mail, calendaring, and contact management. However, the pressure has escalated dramatically based on three industry developments:

- The introduction of the iPad and other tablet devices.
- The resurgence of the Mac.
- The emergence of the Windows-based Ultrabook™ PCs.

Invasion of the tablets
The tremendous success of the Apple iPad caught the electronics industry – and many enterprise IT teams – by surprise. At the point of the third generation iPad’s introduction in March 2012, Apple reported that it had sold over 55 million iPads since its introduction. Based on the iPad’s momentum, as well as more modest success by new entrants such as the Amazon Kindle Fire, analyst firm IDC boosted its 2012 total tablet sales projections from 87.7 million to 106.1 million units in March. This is up from 68.7 million tablets sold in 2011.

Tablets represent a significant new challenge for IT teams, as they are often personally owned but can be used for a wide range of business and productivity tasks. Large numbers of users – many executives – are hungry for easy access to enterprise data from tablets. Meanwhile, IT teams scramble to understand the IT efficiency and security implications of supporting enterprise computing on untrusted devices that are not designed to connect to enterprise data infrastructure.

The tremendous growth of tablet use, combined with the fact that it is driven by user desires and preferences, makes this new flavor of BYOD an unavoidable force for enterprise IT teams.

The Mac is back
Once on the verge of collapse in the mid-1990s, Apple has made a remarkable resurgence to a position as the world’s most valuable publicly traded company. While disruptive devices such as the iPod, iPhone, and iPad drove most of this success, Apple has quietly continued to evolve and grow its Macintosh computer franchise. Following the introduction of the OS X operating system, which combined a pleasing graphical user interface with powerful Unix underpinnings, many technical users such as software developers joined Apple’s traditional audience of creative professionals.

Two additional factors have further advanced the Mac into mainstream corporate computing:

- The “halo effect” of a positive iPhone/iPad user experience may in many cases lead an individual to consider a Mac for the first time.
- Apple pushed the ultra portable form factor boundaries with the introduction of the MacBook Air, resulting in a hardware platform that was very desirable (and trendy) among mobile workers and executives.
Even in cases where Macs are not subsidized the organization, many technology enthusiasts in the workforce are willing to bear the full cost in order to use their platform of choice. Meanwhile, the reality is that many enterprise IT teams have limited experience with the Mac platform.

In cases where Macs are allowed, they are often delivered with a lower level of support by IT, or under a self-service model. In addition, the same major challenge that exists with tablets, coexistence of personal and business content on a single device, applies with user-owned Macs as well.

The rise of the Ultrabook

Based in part on the success of the MacBook Air, the “Wintel” ecosystem has also made a major push into smaller form factor laptop devices, dubbed Ultrabooks by Intel. As part of its Ultrabook initiative, Intel provided an architectural and component framework for ultra portable notebooks to its ecosystem partners.

Major PC manufacturers such as HP, Dell, and Lenovo, as well as design-focused niche players such as Sony and Samsung, are all now shipping ultrathin portables. Even with the Mac’s resurgence, the overwhelming majority of corporate users run Windows. However, even among these users, the emergence of Ultrabooks often increases desire to purchase something other than a standard corporate-issued Windows PC.

While enterprise IT tools and practices have evolved over the last 20 years, there are certain axioms that have remained constant among IT leaders. Topping the list is the tenet that standardization is king. An IT standardization strategy starts with limiting the number of PC platforms in use with the hope that fewer models to support both improves IT efficiency and reduces the number of spare devices and parts that must be kept on hand.

From there, IT teams have traditionally shifted attention to standardizing the software environment. Most large organizations strive to standardize on a “golden image” of a single operating system. Keeping all users on a common image, in theory, reduces IT support cost and complexity. For many enterprise IT organizations, the first order of business upon taking delivery of a new PC is to wipe the factory operating system and replace it with their golden image. In some cases, they even have arrangements in place with their hardware vendor to ship with a custom operating system image.

The final standardization strategy for most IT teams is to limit the changes that individual users can make to their PC. Whether it is change to the operating system settings or installation of an application, any change a user makes is a step away from the goal of a standardized, highly supportable golden image. As a result, many IT teams seek to lock down administrative rights on user PCs by default and deploy only corporate-approved applications through centralized software delivery tools.

While the rationale for standardizing is quite sound in theory, in practice it breaks down in most enterprises. Users have grown more sophisticated and technically savvy in recent years, and the number of available applications has multiplied. The result is a long tail of application requirements for individual productivity or departmental functions that is often untenable for IT teams to manage centrally. The workforce is also more mobile than ever, with laptop users outnumbering desk-based workers in most organizations. This drives increased demand by users for administrative control over their PC for convenience and the flexibility to self-support situations they encounter outside of the office.

Shifting management focus from devices to users, as many organizations do with AppSense products, mitigates some of these standardization challenges. However, there is an even bigger wave that is now crashing down on IT standardization strategies: BYOD. In BYOD environments, IT teams will take one step further outside of their comfort zone to a situation where they have little to no control over the underlying operating system and hardware platform. Further complicating matters is the fact that the platforms in question may be both unfamiliar and poorly equipped to access existing enterprise IT infrastructure.

Embracing BYOD in the Enterprise

Standardization is dead. Long live consumerization.
Along with the loss of standardization, another key IT challenge presented by BYOD is the fact that users are often moving from one to multiple computing devices. In short, the problem is bigger than it seems. It is not simply a matter of a single device per user becoming more complex to manage as a result of lost standardization and higher instances of personal data and applications finding their way into the corporate environment. More often than ever, users will have multiple devices once PCs, smartphones, tablets, and all other computing devices and virtual environments are accounted for. As a result, the overhead of BYOD is often 100 percent additive to existing IT support demands. Moreover, the fact that its driven by users, including executives who do not need to take no for an answer, means that it cannot be avoided.

Every organization is different, and while both IT teams and vendors are reacting to this new and fast-growing challenge, there are no silver bullets. However, in general, a shift from a device-centric management approach to a people-centric IT strategy will prepare enterprises for the reality that most users will be moving between multiple computing environments, each with their own security risk profiles.

There are multiple strategies for enabling trusted corporate computing on the untrusted or unmanaged personal devices. They each have trade-offs, but in the right combination they can help IT teams contend with the unavoidable flow of personal devices into the enterprise.

Remote desktop overlay
Many IT organizations are already investing in server-hosted computing models such as virtual desktop infrastructure and remote desktop session hosts. While the original intent for making these investments may not have been to support mobile devices, the reality is that desktop virtualization vendors such as Citrix and VMware do offer capable remote desktop clients for tablets, smartphones, and Macs.

Some enterprise IT teams use virtual desktop overlay as a “catch-all” solution to the BYOD challenge. Rather than attempting to deliver and support corporate services on an unmanaged device, they deliver no services directly on the endpoint and instead use it purely as a remote client.

The obvious benefits to the IT team are simplicity, security, and control. However, there are also some significant drawbacks. In the age of new computing form factors such as tablets, users are often making conscious decision to use the right tool for a particular job. For example, they may choose an iPad because the native experience on that device is most appropriate for the task at hand. Forcing the user to peck at a remote Windows session from an immersive device like the iPad, for example, is not likely to result in high user productivity and satisfaction.

Enabling a native experience
The ideal situation for most users is to perform both business and personal computing activities side-by-side using the native capabilities and user experience of the device they have selected. Along with above example of an iPad user seeking a touch-optimized experience, a major draw to the Mac platform is the OS X operating system and its collection of applications. While non-Windows users may be willing to use a Windows virtual desktop for certain tasks, they will almost certainly find native applications on their device of choice preferable for many activities.

This presents significant challenges to the IT team. The first challenge is that they often do not directly control the user’s personal device, so it is wise for them to view it as “untrusted.” With devices such as the iPad, there is almost 100 percent certainty that any business activities will be running alongside personal applications and data. In addition, a device like a personally owned tablet or smartphone is much more likely to be passed around among family members and friends, further complicating the effort to secure enterprise data and maintain sound governance.
Embracing BYOD in the Enterprise

A people-centric approach is the answer

While BYOD remains in its infancy, the fact that it is rapidly accelerating as a result of user-generated momentum means that it cannot be ignored. If enterprise IT teams fail to act, users will develop their own solutions, often putting personal productivity ahead of IT priorities such as security and compliance.

There are many tools in the hands of IT teams today, including several from AppSense, which can be applied to formalize a sound BYOD enablement and support strategy. The keys to success are to:

- Use pragmatic solutions such as virtual desktops and session hosts where appropriate while striving to deliver a native device and application experience wherever possible.

- Recognize that no silver bullets exist, but that a shift to a people-centric management strategy will offer to flexibility to evolve and adapt as device usage preferences shift.

- Employ a strategy that combines flexibility to support new user-requested platforms with better control and flexibility of existing Windows-based systems. (They aren’t going away.)

Visit appsense.com/byod to stay up to date on how AppSense is working with the world’s largest enterprises manage the growing BYOD challenge.
About AppSense

AppSense, the people-centric computing company, is the leading global software provider of user virtualization solutions that transform organizations into productive mobile workforces securely governed by IT. AppSense works with customers to reduce IT complexity and enable enterprise consumerization with independent management of the user experience across all mobile devices and desktops. User virtualization improves the deployment, management and migration of multi-platform desktop and mobile environments. The company is headquartered in New York, NY with offices around the world. For more information visit www.appsense.com.