Embracing bring your own device (BYOD)

How to balance user freedom with corporate control

Introduction

The role of the IT department is continually redefined as successive generations of technology force their way into the workplace in response to economic pressure, user demand, and desire for competitive advantage. This has never been more obvious than with the current growth in "bring your own device" (BYOD) programs, which are rapidly spreading through the business world, bringing new headaches and opportunities.

In this paper we're going to consider the three major flavors of BYOD:

- Bring your own laptop
- Bring your own tablet
- Bring your own smartphone

We will look at BYOD from multiple points of view, including the need to balance access (user productivity) with security (corporate liability, data sovereignty, privacy and liability), and we'll make recommendations about approaches that enable you to embrace BYOD in a way that makes sense for your organization.

Bring your own laptop

Anecdotally, "bring your own laptop" started with executives bringing Macs into the enterprise, drawn by the combination of coolness, simplicity and quality that Apple have perfected for a certain class of individual who is willing to spend a bit more and who requires only the out-of-the-box experience. The desire to use non-Windows devices in settings dominated by Microsoft has spread to a much wider population,

especially in the more artistic fields where graduates are familiar with Apple devices from their schooling. Apple penetration into the enterprise has been hard to quantify simply because so many devices are not provided by the enterprise; users are "bringing their own." But in January 2012, Forrester claimed that 21% of information workers use one or more Apple devices in the workplace. Although the iPhone and iPad account for more than half of these devices, Mac OS X is increasingly present as well.

On the PC front, TechTarget's "Consumerization of IT State of the Industry Survey 2012" survey found that more than 60% of companies said that their users connect to the corporate network with personal computers from outside the office, and more than 40% of companies do the same from inside the office.

This is a classic example of user demand and consumerization bypassing corporate IT in the name of getting things done. The fact that so many of these devices were introduced by executives who could override corporate policy and just demand that they be connected and supported was key in forcing the acceptance of "Bring Your Own Mac" in many organizations. Sure, some organizations do provide Apple devices for a subset of their users, but usually only in very specific use cases.

Benefits and risks of "bring your own laptop"

So what are the benefits of "Bring Your Own Laptop," and what are the risks?

The benefits include:

- **Enhanced user productivity** – Happy users work longer and harder. Using a familiar device that suits their tastes and needs encourages them to contribute their individual talents and personality into your organization. Attracting talented, free-thinking employees is easier in a workplace with progressive policies and forward-looking IT policies.

- **Predictable hardware costs** – If your organization pays a fixed stipend to employees and allows them to purchase and use their own devices, then, theoretically, it can predict its expenses more accurately. Of course, employees might not purchase devices that support corporate applications or meet other requirements for them to be productive, and they are less likely to keep their devices up to date when the money comes out of their own pocket.

- **Lower support costs** – If your organization puts the burden of purchasing and maintaining laptops onto its users, then the help desk has, in theory, less to do. Moreover, since users are able to bypass IT so easily and provide services – such as email, web hosting, CRM, document backup, and collaboration – for themselves, managing endpoints is a hopeless task anyway, right? This is, of course, a controversial and extreme viewpoint, but advocates of consumerization are convinced this is the future. (They are, of course, all highly self-sufficient IT people who would never phone a help desk anyway.)

The risks include:

- **Lower user productivity** – Corporate IT has provided a standard class and build of laptop for years because they know it will support the work environment. As soon as users bring their own mix of hardware specifications, operating systems and applications into the workplace, you can't predict how productive they can be, especially remote employees with no local IT presence. One of the biggest problems is application compatibility, since many business-critical applications are still tied to Windows, and often only one version of Windows.

- **Liability** – With corporate data knowingly stored on devices that are owned by individuals, we are in murky legal water. If customer data, records, blueprints, trade secrets and other protected information are stored outside corporate control and policies, then suppliers, customers and

In January 2012, Forrester claimed that 21% of information workers use one or more Apple devices in the workplace. Although the iPhone and iPad account for more than half of these devices, Mac OS X is increasingly present as well.

DELL

partners could rightfully be concerned about privacy and data theft.

- **Higher support costs** – When laptops owned by employees break down, the employees will take their machines to the Apple Store – or call the corporate help desk? Now IT is burdened with supporting a nearly infinite matrix of hardware devices and operating systems.

- **Higher software application costs** – Applications cost significantly more on some platforms than others, and tracking software licensing usage outside the corporate domain on user-owned devices has extra challenges. Anecdotal evidence suggests that software licenses will be over-provisioned more, and average per-user costs will be higher in a BYOD model.

Recommendations

The obvious goal is to maximize the benefits while minimizing risks. A number of technologies offer some real answers, enabling you embrace "bring your own laptop" in a safe, productive manner. You can:

- Explore virtualization.
- Extend your endpoint management solutions to BYOD laptops.
- Enforce security policies based on location and access point.

Explore virtualization

There are two main approaches to virtualization, server-hosted and client-hosted:

- **Server-hosted desktop virtualization** – Windows applications run in the datacenter, with remote display onto any device, over pretty much any connection. This approach requires that the user has a continuous connection across the network or Internet, but it solves all kinds of BYOD problems by ensuring that data and applications never leave the datacenter and therefore can be strictly controlled. This technique can also be used on pretty much any device.

Server-hosted desktop virtualization comes into two variants:

- **Session virtualizatio**n (a.k.a. Terminal Server), in which every user gets an isolated slice of a Windows Server in which to run their applications. This is more economical and more widely adopted than the alternative, desktop virtualization.

- **Desktop virtualization** (a.k.a. VDI), in which every user connects to a Windows client operating system running in a virtual machine. VDI offers greater isolation, and improved hardware and application compatibility, but comes at a higher price in hardware and licensing.

- **Client-hosted desktop virtualization** – A sandboxed virtual machine is placed on a user's laptop, centrally secured and managed, and synchronized with the data center periodically. This approach has the advantage of continuing to work when no network connection is available, and can also offer better graphics performance than server-hosted desktop virtualization because all graphics display traffic runs locally inside the computer. However, the client-hosted approach works only on laptops with enough power to host a virtual machine, so it typically requires 2 GB or even 4 GB of RAM, and only the best solutions support Mac as well as Windows.

It is worth noting that there are two approaches to client-hosted desktop virtualization:

- **Type 1 hypervisor**, in which a thin micro-OS runs on the hardware and manages all the virtual machines. There have been numerous attempts to achieve this while balancing feature complexity with low resource consumption, but the biggest drawback is that this approach requires users to wipe their laptops clean and start over.

- **Type 2 hypervisor**, which runs inside a host Windows or Mac operating system.

The obvious goal is to maximize the benefits while minimizing risks. A number of technologies offer some real answers, enabling you to embrace "bring your own laptop" in a safe, productive manner.

This approach requires more hardware resources on the host and theoretically delivers lower performance than the type 1 hypervisor, but it does not require users to wipe their laptops clean and so is better suited to a BYOD program.

Extend your endpoint management solutions to BYOD laptops

Most organizations already have a management solution for looking after Windows laptops and desktops that takes care of tasks such as software deployment, inventory, patch management and operating system imaging. Examples of these tools include the KACE K1000 and K2000 appliances, Microsoft System Center Configuration Manager, and solutions from Altiris and LANDesk. Where these tools do not natively support non-Windows devices, other products can help; for example, Dell Management Xtensions for SCCM extends the reach of System Center to Apple Mac OS X desktops and laptops.

The challenge is that some of these solutions can fully manage only endpoints that are joined to an Active Directory domain, but users who bring their own laptops will be reluctant to surrender them to the IT department. This situation should be familiar to anyone who has managed smartphones, which cannot be domain-joined; to help, products like Exchange ActiveSync have incorporated features to force security policies onto devices before allowing them to connect to corporate email. The new direction of endpoint management is further evidenced in the Windows RT devices being released alongside Windows 8. These consumer-focused devices cannot be domain-joined, but Microsoft has answered enterprise requests for management capabilities with a new self-service portal. It allows for application subscription and deployment, and also enforcement of some security policies on the device, so that only devices which conform to controlled security standards have application access.

As domain-based management (built on explicit trusts and named accounts) evolves into claims-based security (built on federation), device management will increasingly not be built around domain membership.

Enforce security policies based on location and access point.

Regardless of how you allow access from user-owned laptops in a BYOD program, you need to consider the level of access to corporate applications and information that will be available based on your users' locations and their access methods. For instance, users in a secured workplace on an encrypted network connection should have significantly more access than users working from home on an untrusted connection. There are a few possible approaches:

- Desktop virtualization policies – As we have seen, desktop virtualization is well-suited for BYOD and offers exceptional control in both the client-hosted and server-hosted forms. Both approaches allow control based on user location (IP range), access type (e.g., whether two-factor authentication was used), group and OU membership, device type and much more.

- User environment management – Solutions that manage the user's environment inside the operating system can restrict the type of data that a user can see and the applications they can run based on all kinds of environmental settings.

- Identity and access management – At a directory and network level, there are security solutions that control user access across all systems and provide a holistic approach to user provisioning and privilege levels. This extends beyond just application and device management into the whole world of user management and security. Advanced solutions in this space provide very fine-grained policies and integrate into all other IT and network systems.

> Regardless of how you allow access from user-owned laptops in a BYOD program, you need to consider the level of access to corporate applications and information that will be available based on your users' locations and their access methods.

Bring your own tablet

The sudden explosion in demand for tablets remains something of a curiosity – tablets have existed for years and have been used in medical, warehousing and delivery services successfully, but it wasn't until Apple cracked the combination of long battery life, touch interface, slim dimensions and an indefinable coolness that it became a must-have item, especially in the consumer market. The simplicity and convenience of the iPad transformed the human-computer interface and experience for reading, browsing and game play, and surprised everyone in how quickly it became an essential addition to the list of gadgets needed for modern life.

Android-based tablets offer many of the same benefits but have not attracted the same demand for various reasons, and with the imminent release of Windows 8, Microsoft is getting into the game, even going against its traditional business model and selling its own brand of hardware devices.

With users so attached to the tablet experience at home, it is no surprise that they want and expect to use them in the work environment too. The question, once again, is whether bringing this new wave of consumer-owned devices into the workplace should be permitted and/or encouraged.

Benefits and risks of "bring your own tablet"

The benefits of "bring your own tablet" include:

- **Extended working** – The most obvious appeal of tablets is the flexibility and comfort they allow in working with applications – for lounging in a chair, working on a plane, or even while mobile in the workplace, the tablet is far lighter and more convenient to carry than a traditional laptop. If corporate applications and data are available on tablets then users are able to work at times when they would normally be unproductive.

- **Greater flexibility** – A laptop is too complicated and too unwieldy for many people, but a tablet puts their most frequently needed computing tasks into a consumer device with a perfect form factor that can go anywhere. By allowing the use of tablets alongside other user-owned computing devices, your organization can maximize the number of ways its users can work in and out of the office, and in a style that suits them better.

The risks include:

- **Security** – A lost tablet, like a lost laptop, is a risk if it exposes sensitive data or allows unauthorized access. However, the risk is somewhat lower for tablets since it is unusual to store much data on a tablet.

- **Liability** – As discussed with BYO Laptop, the use of a user-owned device in a corporate setting can create legal complications, especially if the organization has a lot of sensitive or privileged data. The risk is lower for tablets, since data is consumed but rarely stored on a tablet, but the fact that data is used on a personal device might breach contracts, regulations or privacy laws.

- **Increased support costs** – For all their simplicity, tablets can still generate support calls if users cannot get secure connections or if applications do not work correctly on their particular tablet. Tablets are generally used in addition to other computing devices, not as replacements, and so the likely effect is an increase in support demands.

Recommendations

For a successful "bring your own tablet" approach, you should:

- Explore virtualization
- Enforce security
- Consider mobile device management (MDM) solutions
- Check application compatibility, both web and native

> The simplicity and convenience of the iPad transformed the human-computer interface and experience for reading, browsing and game play, and surprised everyone in how quickly it became an essential addition to the list of gadgets needed for modern life.

DELL

According to Information Week 2012's Consumerization of IT survey, 63% of organizations allow email access from personal smartphones, up from 58% in 2010.

Explore virtualization

Virtualization presents corporate Windows applications securely on user devices, and therefore offers the same benefits for tablets as discussed earlier for laptops. Virtualization provides control over data storage and location, and existing applications can be delivered to all tablet users immediately. In some ways, the tablet is the perfect thin client since it is designed from the ground up as a consumption device.

However, there are some considerations unique to tablets:

- The touch screen interface will not be suitable for many Windows applications. There are tricks and tools to make a Windows application more usable on a touch screen tablet, but the user interaction is fundamentally different and will not be suitable for all apps.

- Client-hosted desktop virtualization is not an option on tablets because they don't have sufficient computing power or RAM to run a locally hosted virtual Windows desktop, and the CPU is generally not x86/x64 architecture.

- With at least four major tablet platforms in the market (Apple iPad, Android, Windows RT (ARM), and Windows 8 (x86)), application compatibility is a problem. Apps that are available for one platform might not be available with the same functionality on the others, if it is available at all. Virtualization ensures a Windows application works the same on all tablets.

Enforce security

Simple steps, such as forcing the use of passcodes when connecting to corporate resources like email, can help prevent unauthorized access if a tablet is lost or stolen. It is also a good idea to change log-on credentials whenever a tablet goes missing.

Consider mobile device management (MDM) solutions

In the "bring your own smartphone" section below, we will look at MDM a little more. Because many tablets run a operating environment that is similar to smartphones, they fit will into many of the same management solutions. For example, solutions for managing, tracking and securing iPhones work equally well on iPads.

Check application compatibility, both web and native

If you have a particular application that users rely on, before encouraging use of a tablet version of that app, make sure it is available on all the target tablet platforms and that it offers all required functionality in each native version. If no native version of an app is available, consider virtualizing a Windows application.

If you are using web apps, which are displayed in a browser, check whether a mobile version is available and works well in all target laptops and in mobile browsers. It might be that the web app works correctly only in a "full" browser, or that it requires ActiveX plugins and the like, in which case virtualization is the only answer.

Bring your own smartphone

Finally we turn to the new wave of mobile communication devices with amazing computing power and con-nectivity speeds. Using smartphones for accessing corporate email is easily the most widespread and accepted form of BYOD, and with the ability to force use of passcodes and the limited storage on smartphones, it is probably the least risky.

According to Information Week 2012's Consumerization of IT survey, 63% of organizations allow email access from personal smartphones, up from 58% in 2010. However, research from Coalfire suggests that even the most basic security measures are often not enforced: 84 percent of individuals stated they use the same smartphone for personal and work usage, and 47 percent reported they have no passcode on their mobile phone!

Recommendations

Recommendations for a successful "Bring Your Own Smartphone" strategy include:

- Enforce security
- Limit virtualization
- Test web apps for compatibility with mobile browsers
- Check smartphone apps for missing features

Enforce security

A wide range of mobile device management (MDM) vendors offer tools for tracking and securing mobile devices, and many offer features like file synchronization, app sandboxing and secure network tunnels for corporate data. The Gartner Magic Quadrant provides a good survey of the current major players. Over time, we expect to see more and more MDM features included in the major endpoint management solutions from Dell, Microsoft, Symantec and others.

Limit virtualization

The small screen size of smartphones limits the types of applications that yield a good user experience. Although smartphone apps for accessing virtualized Windows desktops and applications exist, their usefulness is limited. Smartphones are best suited to simple email clients and mobile-friendly browser applications, where a subset of key functions is presented in a format suitable for touch-based small screen sizes.

Test web apps for compatibility with mobile browsers

If no mobile version of a web site or web app is available, it might still be possible to use the web site or app on a smartphone using the native browser, but expect compatibility and performance issues. Solutions are coming onto the market to automate testing in these situations, but user acceptance testing is still going to be a manual task. Try alternative browsers such as Opera if the built-in browser just isn't getting the job done.

Check smartphone apps for missing features

Many business solutions have native smartphone apps for the most popular iOS and Android platforms, but they usually offer only a subset of functionality. Try before you buy! Just because there's a check in the "iPhone client" box, don't assume it will give you all the features you need.

Conclusion

To end users "bring your own device" appeals as an unprecedented opportunity for flexibility and productivity. To IT it can seem like a security and compliance nightmare. The reality is that BYOD –which includes laptops, tablets and smartphones – offers both benefits and risks. By following the recommendations in this paper and taking advantage of technologies available on the market, you can implement an effective BYOD policy that achieves an appropriate balance between user freedom and corporate control, maximizing BYOD benefits while minimizing its risks.

Wyse vWorkspace

vWorkspace is a desktop virtualization and application delivery solution that complements native Microsoft technologies to provide a platform that is not only simple, scalable and extremely flexible - but one that also delivers enterprise-class performance.

Simple to install and use

vWorkspace requires no dedicated specialists for deployment and ongoing management of the infrastructure. Built on mainstream Microsoft technologies, organizations with existing experience in Remote Desktop Services (RDS), Hyper-V and System Center will find vWorkspace to have a familiar structure. The vWorkspace management interface is designed with the desktop professional - rather than the server professional - in mind, and is therefore geared toward those activities most common to desktop management and application delivery. End-to-end monitoring and diagnostics provide deep visibility into the complete, desktop virtualization infrastructure - all the way down the individual user experience. Simplicity, paired with a robust feature set and exceptional technical support have helped vWorkspace maintain a customer satisfaction rating greater than 90%.

Scalable and flexible for organizations of all sizes

Whether tens of thousands of employees or five employees, vWorkspace scales up and down, down and up, based on your requirements. vWorkspace flexible profiles enable very granular resource assignment that can be custom tailored to each user based on seemingly endless combinations of over twenty parameters including such things as IP address, location, device type, organizational unit, day of week, time of day and many more. And with increasing interest in desktops hosted in the cloud, it's also important to note that vWorkspace also supports multi-tenancy to meet the strict requirements of managed service providers.

Enterprise performance

Paired with Hyper-V, vWorkspace enables the deployment of thousands of desktops in under an hour. Install or upgrade to a new version of Windows across all of your desktops in twenty minutes. In addition, users will enjoy a rich, "like-local," experience leveraging native Microsoft RemoteFX optimized on Dell infrastructure and clients.

Learn more about vWorkspace

About Dell

Dell Inc. (NASDAQ: DELL) listens to customers and delivers innovative technology and services that give them the power to do more. For more information, visit www.dell.com.

Dell cloud client-computing

One Dell Way
Round Rock, TX 78664
www.dell.com

Refer to our Web site for regional and international office information.