GREEN HOUSE DATA

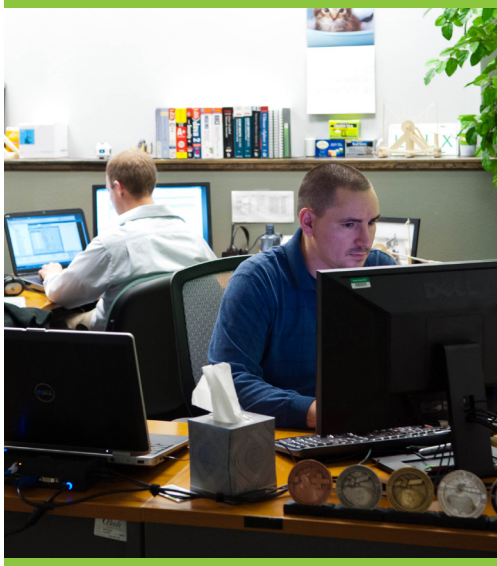
Built right. Just for you.

WHITE PAPER

4 Steps to Secure BYOD

Using Virtual Desktops To Increase Productivity Without Increasing Risk

Presented by Green House Data



greenhousedata.com

Green House Data
304 Progress Circle
Cheyenne, WY 82007

Introduction

Bring Your Own Device, or **BYOD**, has been an emerging trend in the IT world for years and has hit full buzzword status. With BYOD, employees use their own mobile devices (smartphones, tablets, or laptops) for work functions. It's more than a fad. One survey found 60% of full-time employees were using their personal devices to access corporate data. BYOD continues to grow with or without the support of IT departments, with 21% of employees using their own devices despite an anti-BYOD policy[1].

This sometimes-unauthorized use of personal devices opens up a big can of worms for IT, namely security woes, especially in heavily regulated industries like healthcare or banking. Ultimately, employees will use their own devices for work functions, and IT departments must decide between the security risks of unmanaged mobile platforms and the dedicated budget and time required for virtual desktop implementation.

A combination of virtual desktop infrastructure, mobile device management, and other tools can help IT departments manage the influx of personal devices used in the workplace. This white paper will examine the initial considerations and steps to take when weighing BYOD policy, software options, employee training, and security or compliance standards.

1) Decide If Mobile Support Is Worthwhile

The first step to take is to decide whether a virtual desktop infrastructure or mobile device management system is worth the expenditure. These systems can initially seem expensive, especially when deploying in-house solutions. They require tricky software licensing—Microsoft has hundreds of options alone, depending on whether users need persistent desktop states and other factors. Employee training, IT support, and adding resources to infrastructure to ensure a smooth experience are all vital to the success of BYOD adoption, and add significant costs. Some companies might also consider reimbursing their employees if they buy supported devices, but according to a 2013 Intel survey, most companies aren't doing so currently[2].

1. http://www.itpro.co.uk/mobile/19944/surge-byod-sees-710-employees-using-their-own-devices

2. http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/consumerization-enterprise-byod-peer-research-paper.pdf

Benefits of VDI

VDI is a simple concept: deliver a standard desktop experience with dedicated resources regardless of user hardware. It has far reaching benefits, however, and depending on your company needs it can help:

- Meet compliance standards for security and user access
- Increase productivity
- Minimize the licensing needed for large operations and temporary workers
- Simplify desktop management with single-point patching and updates
- Reduce security risks from unmanaged mobile platforms

Infrastructure as a Service (IaaS) and managed IT from a service provider can mitigate these issues. While managed virtual desktops are also a recurring cost, for smaller IT departments in particular, the less strain the better. In addition, compute resources can be scaled on demand without expensive in-house provisioning.

The benefits of BYOD and mobile support should also be weighed. Virtual desktops can lead to increased productivity, lower OpEx with simplified desktop management, and less spending on hardware provisioning. IT can apply updates across the entire environment with the push of a button. Support times are dropped as a simple reset of a virtual desktop fixes the vast majority of issues.

2) Employee Awareness and Mobile Device Policy

This step can be taken alongside the cost-benefit analysis, as surveys and examination of previous policies will give vital insight into the current state of mobile usage at a company.

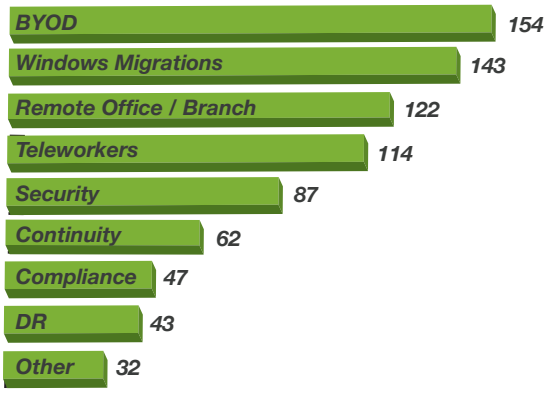
Companies launching a virtual desktop environment and offering support for mobile devices must have a detailed **mobile use policy**, if not several dedicated to different employee roles, for security and legal purposes. Remote access policies of the past tend to be based on PCs and do not consider modern smartphones and tablets.

Policies must be overhauled and understood by the entire organization so there is no infighting about help for unsupported devices. Be prepared to limit support and types of data delivered to personal devices based on realistic estimates of manpower. Gather old policies from various departments and different technology groups to create a unified new front.

Survey current usage to see what platforms and devices are commonly used—if employees are reluctant to provide information, set a date when you will reset their connections to e-mail forwarding, or use another effective cutoff. Collect information on OS version, company vs. employee ownership, what kind of data is transferred, applications, authentication, and entry paths like cellular, Wi-Fi or VPN. Based on this previous information, design a matrix for different employee roles describing what devices will be fully, partially, or not supported.

> *Employees increasingly expect support for their devices, applications and cloud services.... Most importantly, they are bringing this technology into the workspace, regardless of organizational policy.*
>
> ***Gartner, April 5, 2013***
> ***"Cutting Through the Myths and Realities of BYOD and HVD"***

Figure 1
Priorities When Considering Deployment of HVD (percentage of respondents)



Source: Gartner, April 2013

3) Evaluate VDI and Infrastructure Options

There are a variety of virtual desktop delivery products available for in-house deployment or third party management. Considerations must include user authentication, security and compliance measures, and application delivery.

The major players are **VMware Horizon View**, **Citrix XenServer**, and **Microsoft Server**. Amazon Web Services has recently thrown their hat in the ring with Workspaces. Most of the features are very similar across the board, with included firewall management and network security policies. The largest differences come in the number and type of servers and storage supported, API availability, bare-metal support, and management portals. Companies will have to do their own evaluation as to what features are important, but in the end the decision will likely rest on integration with existing systems.

Deployment options will be based on the mobile policy draft and depend on worker roles. Desktops can be stateless, stateful, or designed for power users. Stateless workstations will boot to a standardized desktop and will not save personal information or allow application installation. They have limited access to specific applications and are ideal for shared computers or contract employees. Stateful desktops allow some personal information to be saved and require additional licensing. Power users have a separate VM master image and have a more granular level of control and

> *"Compliance regulations are considered a primary barrier... Companies in heavily regulated industries have concerns about their ability to guarantee data security.*
>
> ***Intel, 2012***
> ***"Insights on the Current State of BYOD"***

network access including installing applications. Windows 7 and 8 desktops can be easily deployed across the major VDI platforms. VMware Horizon View and Citrix XenServer can deploy Linux desktops as well, and provide support for many user devices and operating systems including iOS, Android, Windows, and MacOS.

Depending on the expected usage levels, companies may need to increase their compute resources to install an effective VDI. This can be done in-house through time-consuming hardware provisioning or quickly added via hybrid or private cloud IaaS. Virtual desktop service packages come in scalable sizes. A typical offering may look like:

VIRTUAL DESKTOP ENVIRONMENTS			
Size	**CPU**	**RAM**	**HDD**
Small	2 vCPU	2GB	40GB
Medium	2 vCPU	4GB	40GB
Large	4 vCPU	8GB	120GB

If partnering with a service provider, VDI packages may come preinstalled with productivity tools and applications. Microsoft Office and Exchange, Adobe Reader, various antivirus tools, and web browsers are all common installations. Backup as a Service and managed security are common add-ons as well.

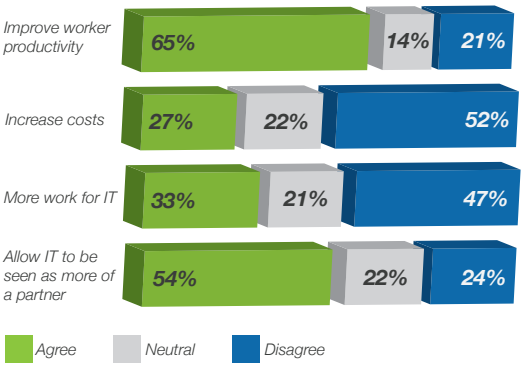
4) Implement Mobile Access Security

Time to put new mobile policies to work through an opt-in portal on first sign-in or a physical document signed by all users describing acceptable use and risk mitigation. Deny access to any devices without up to date patches, an antivirus selected from an approved list, or without a remote wipe agreement. Horizon View and other virtual desktop software makes it simple to push updates and antivirus to all desktops, but the user-end device must also have the necessary security precautions. Connecting through the official company **virtual private network (VPN)** should be a requirement; all connections outside the VPN should be put in a separate limited access group or else denied access all together.

If your infrastructure doesn't meet compliance requirements, service providers can set-up a compliant mobile desktop environment depending on their certifications. Healthcare providers can reap some of the biggest benefits of BYOD, allowing mobile care providers access to electronic health information while maintaining compliance. But this industry in particular needs strict data security measures on all network connections. The most frequent source of breaches is lost or stolen equipment, so **remote wipe** is a vital tool for mobile security.

Figure 2

IT Professional Survey on the Impact of VDI



Source: Intel, October 2012

The essential ingredients to a safe remote desktop environment are **user authentication** and **secure socket layer (SSL) security certificates**, two cornerstones of network security. Monitoring tools can collect network logs and watch for suspicious activity, like rapid login attempts. **Network access control (NAC)** software can be combined with **mobile device management (MDM)** tools (make sure to evaluate compatibility before installation) to keep policies in place regarding necessary user security and network settings. The required settings that should be considered include up-to-date **patches**, approved and up-to-date **antivirus**, **disk encryption**, and **port blocking**.

Conclusion

Make no mistake: whether updating an old BYOD policy or implementing new mobile management tools, this can be a large undertaking. However, virtual desktop infrastructure can provide a secure portal for mobile users, enabling higher productivity on the user side and better security, management, and insight on the IT side. With careful planning, the proper tools, and maybe an infrastructure services partner, small-medium businesses and enterprise companies alike can reap the benefits of VDI and solve BYOD woes at the same time.

About Green House Data - Green House Data provides VMware powered cloud hosting and colocation backed by 24/7 live support. Headquartered in Cheyenne, Wyoming, the company has data centers in Cheyenne, Portland, OR, and Newark, NJ. The facilities are HIPAA and SSAE 16 Type II compliant, powered entirely by wind and solar power, and designed to be 40% more energy efficient than comparably sized data centers.

Wyoming Office
304 Progress Circle
Cheyenne, WY 82007

Denver Office
110 16th St, Suite 1240
Denver, CO 80202

T: *866.995.3282*
F: *307.316.0404*
E: *info@greenhousedata.com*

Technical VDI Challenges

Virtual desktops aren't without their difficulties. One major concern is "**bootstorms**", when many users log in at once, often at 9:00 AM on a workday or for large meetings. Antivirus storms are similar, when scheduled scans begin on virtual machines across various servers. Bootstorms put significant strain on network architecture and virtual machine resources, leading to slowdowns, freezing, or otherwise unsatisfactory user experiences.

Storage is perhaps a larger obstacle than network latency or the overload of many simultaneous users, as compute resources are relatively easy to scale while storage is more expensive and chewed up at a quicker rate. This depends on whether you deploy stateful or stateless virtual desktops, allowing users to save their personal information or not. Specially designed storage arrays can help ease storage performance issues.