

# INSIDER'S GUIDE TO Hybrid IT Environments: Pros, Cons and Best Practices

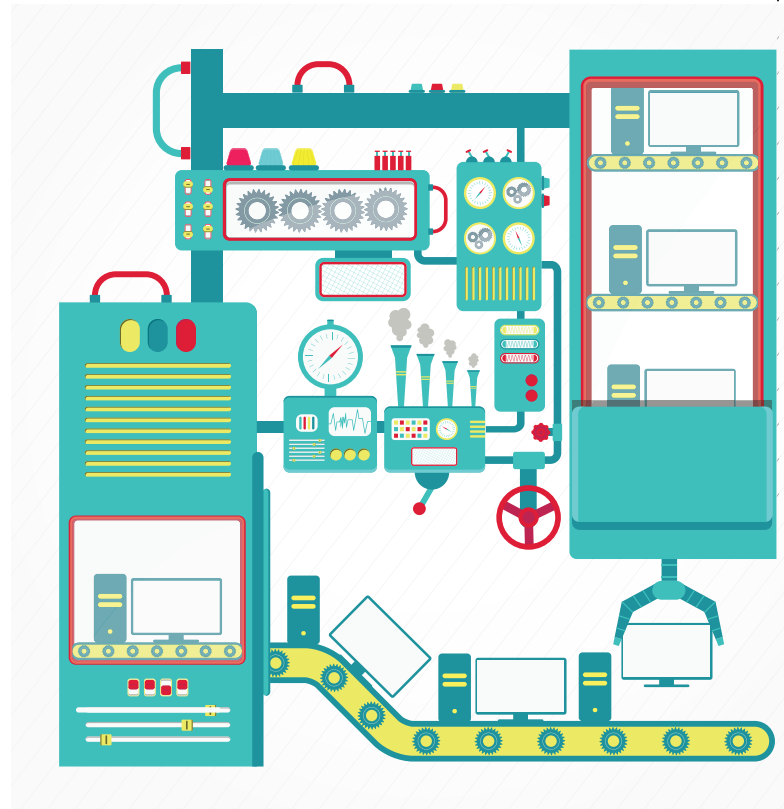
There are good reasons to have both Linux and Windows running on your network. The downside is the potential management and boot headaches. This guide digs into the details of running both OSES for the greatest efficiency and performance.

**W**indows and Linux might be mortal enemies in the marketing arena, but in many real-world operating environments, IT professionals have to be ready to address both. A developer could benefit from testing on both platforms before introducing a software product to the masses. An employee might need to launch an essential open source application that isn't Windows-friendly. Systems admins might be using stripped-down Linux distros to save money on network monitoring or logging chores. These objectives and more can be achieved in an environment that harmonizes these independent OSES.

A heterogeneous infrastructure is a dream scenario for IT geeks who crave the best of both worlds: the familiarity and user-friendliness of Windows, plus the flexibility and control of Linux, all at your fingertips. As for how to go about carving out this ideal IT environment, you pretty much have two options: dual booting or virtualizing.

## Dual Boot vs. Virtualization

Virtualization technology gives you the power to transform your main OS into a platform



that hosts a number of guest systems as virtual machines (VMs). It doesn't discriminate, either, so if Windows 8 is your main system, you can designate a couple of those guests to Linux distros you reserve for testing or other applications you don't want disrupting your core operations. If you're running Linux, you can spin up a VM to experiment with Windows 10 and run both simultaneously while making your assessments.

By nature, virtualization offers what looks and feels like a more seamless transition into hybrid IT. Switching between systems requires no reboot and a few simple configurations make it possible to display their output on two or more monitors, and control each platform with the same keyboard and mouse. IT managers benefit from the fact that you can effectively man a fleet of OSES without ever having to leave

## Running Windows and Linux side by side is essentially doubling your trouble, because you expose the network to an additional set of inherent security threats.

the environment you feel most comfortable in. But there are drawbacks to consider. The limitations of virtualization will ultimately determine how smoothly a given hybrid environment will run. So if your primary OS is acting screwy, there's a good chance that your secondary systems will feel the pain. Vendors can tout superb performance all day, but every VM puts a considerable strain on the host machine. And because there's no direct access to the hardware, 3D rendering and other resource-intensive applications can be problematic.

Dual booting is something IT admins often encounter during their first Linux computer crisis. A dual boot takes place when you configure your loading sequence to boot specific partitions. This is your opportunity to customize your IT environment with the versions of Windows and Linux you want to run on the network. Dual booting offers the advantage of independence; each system runs independently from the other and has direct and exclusive access to hardware resources, so performance is noticeably better.

The trouble with dual booting is that it isn't as seamless as virtualization. For starters, you have to restart the machine to boot each individual OS. I don't know about you, but waiting for a system to load is one of the most agonizing parts of computing in general. Imagine having to do that every time you need to get something done on either platform. And because you have to run them independently, simple, yet critical tasks like updating and patching can become a nuisance.

### Pro Tips on Hybrid IT

As the world turns, the enterprise loses more control over its most critical information technology systems. At one time, IT was able to keep close tabs on exactly which applications

were installed and running from end to end. Things are a bit different now that the modern enterprise is catering to a diverse range of devices running a variety of OSES. Here are some recommended best practices for keeping a hybrid environment running smoothly.

### Get Automated

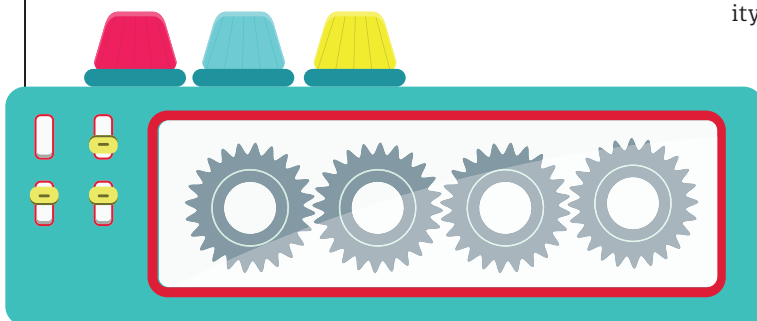
An environment with diverse OS platforms demands a lot in the way of financial and physical resources. Automation technology offers a way to offset the cost of hiring and training new employees to maintain each individual system. IT can use automation to help maintain heterogeneous infrastructure in several key areas:

- System configuration
- Security audits
- Remote app installation
- Help desk administration
- Patch management
- Backup and disaster recovery

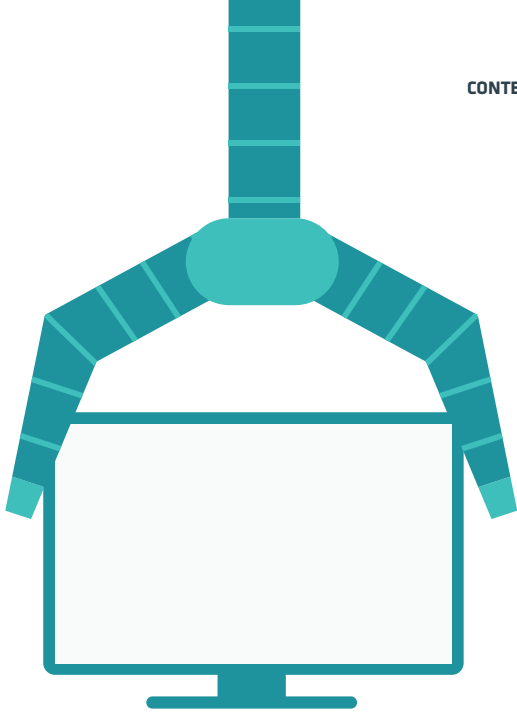
In addition to eliminating systemic pinch points, automation also frees IT staff up to focus on other technology objectives that help move the business forward.

### Grab Some Cross-Platform Tools

A toolkit made of cross-platform IT tools is a must-have for mixed infrastructures. Platform-specific tools might be great at taming the systems they're designed to manage, but are often limited when deployed in a heterogeneous setting. While you sometimes have no choice but to go with a solution that's optimized for a single platform, there are other options that offer cross-platform capability. Look for ones that provide backup and disaster recovery.



Dual booting is something IT admins often encounter during their first Linux computer crisis.



**Platform-specific tools might be great at taming the systems they're designed to manage, but are often limited when deployed in a heterogeneous setting.**

ery with automated functionality that simplify your hybrid IT environment.

### Run Network Inventory

Diligent IT administration means taking inventory of your network like you would for a physical product line. Through this process you come to learn exactly what's on the network in terms of applications, services and data. Consider it a first crucial step toward end-to-end security. This is the point where you decide what's allowed on the network, how to spot untrusted applications, and what to do with anything that isn't company-approved.

### Beef up Security

Running Windows and Linux side by side is essentially doubling your trouble, because you expose the network to an additional set of inherent security threats. Though you want your mixed infrastructure to be as cohesive as possible, bulletproof endpoint security means creating a comprehensive strategy for securing each individual system.

This layered approach should incorporate established security technologies such as VPNs, DDoS protection, firewalls, anti-malware software and encryption, to name a few. Finally, you need tools that enable IT personnel to effectively implement these technologies and policies across your OS pool.

### Stay Up-to-Date

Mixing platforms can make it more challenging to keep your IT systems up-to-date. Technology moves at breakneck speed,

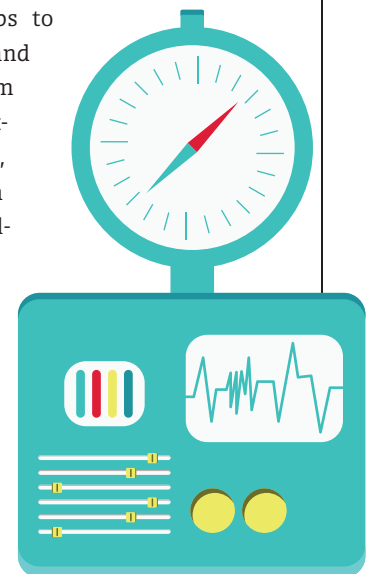
but you don't necessarily have to upgrade every time your vendors roll out a new release. Still, it's important to maintain a comprehensive application roadmap so that you're prepared to move up when it makes technical and financial sense for your business.

The most successful IT administrators monitor their vendor roadmaps to keep track of upgrade dates and paths for each critical system and application. Of all the software in the network ecosystem, your system administration tools should definitely be advanced enough to support

**The limitations of virtualization will ultimately determine how smoothly a given hybrid environment will run.**

your OS mix as updates and upgrades are rolled out.

Hybrid systems are here to stay, and managed services providers in particular will continue to see more and more situations where they'll be called upon to provide cross-platform monitoring and management. Without the right tools, today's complex blend of desktop, server, and mobile OSes can put a strain on IT departments in a way that not only drains corporate budgets, but also taxes technical staffs to their limits. It's up to IT leaders to integrate automation and other technologies that streamline systems management, so they can get the most from these hybrid infrastructures. [VR](#)



# UNCOMFORTABLE



# COMFORTABLE



Having your feet to the flames because of an IT disaster is a quick way to lose time, money, and your reputation. The last thing you want is a painful trial by fire. But using the StorageCraft® Recovery Solution,™ you'll know you can quickly, easily recover from any type of disaster. With trouble miles from your mind, "feet to the flames" will really mean fuzzy socks and hot cocoa. How's that for comfort?



Follow the link, or scan the QR code to see how StorageCraft helps make MSPs feel all warm and fuzzy.  
[www.StorageCraft.com/warmandfuzzy](http://www.StorageCraft.com/warmandfuzzy)

StorageCraft and Recover-Ability are trademarks or registered trademarks of StorageCraft Technology Corporation.  
All other brands and product names are trademarks or registered trademarks of their respective owners.

STORAGECRAFT.  
**RECOVERY**  
SOLUTION™