Managing Multiple Operating Systems: Five Best Practices

By Tim Clark
The FactPoint Group

Table of Contents

1.0 Introduction

No longer does IT have the luxury of exercising full control over what operating systems can be used in the corporate setting. Until a few years ago, IT decided not only on operating systems but also on which applications could be installed on endpoints. But today the scenario has significantly changed with multiple operating systems making inroads into the enterprise space, running on different devices with different form factors. With so many options, today's organizations and users are moving away from a PC-only model to a more diverse approach that embraces multiple devices running on a variety of platforms. Beyond desktops, corporate IT must now support mobile laptops, tablets, smartphones and other consumer technologies. Thus IT must be equipped to manage multiple operating systems in an efficient, scalable and secure way.

This paper will address enterprise IT trends that are forcing IT departments to broaden what they support. It also will present five best practices for tackling the growing issue and detail how the Dell KACE K1000 Management Appliance addresses both IT trends and best practices.

2.0 Enterprise IT challenges

2.1 Windows 8

The biggest looming change is the release of Windows 8,[1] now expected in October 2012. Windows 8's imminent arrival was blamed for slower PC sales in summer 2012 as companies and individuals waited to buy new machines that have the new operating system already installed. The pattern is not uncommon for major Windows releases and Gartner Inc. projects that by 2015, Windows 8 will reach 60% of the customer base and account for 93% of PC shipments.[2]

For IT departments, the release of Windows 8 will put a premium on IT tools that can support established operating systems while being able to easily scale to handle this new operating system the moment it ships. While some buyers are waiting to refresh their systems with Windows 8, others are buying new machines running Windows 7 with the intent of upgrading them later. Tools that help IT manage such upgrades will also be prized.

Windows 8 is considered to be a game changer for IT because it allows systems administrators the ability to manage laptops, desktops and tablets in a consistent way instead of using separate solutions for each of these devices. If Windows 8 delivers a good user experience, IT organizations might favor Windows 8-based tablets over Apple iPads simply because the existing enterprise-ready Microsoft ecosystem can help to incorporate Windows-based products so they work together seamlessly.

[1] Windows 8 will come in two flavors: Windows 8 on x86/64 (for desktops, laptops and tablets powered by x86 processors) and Windows RT (for PCs and tablets powered by ARM processors). Both Windows 8 on x86/64 and Windows RT support the Windows desktop experience.
[2] "Forecast: PC Market by Operating System, Worldwide, 2011 Update," Gartner Inc., by Annette Jump, C.G. Lee, July 1, 2011, ID:G00214411.

2.2 Tablets

Tablets are increasingly popular with consumers and companies as either the primary or the secondary computing device because they are conveniently portable and offer comprehensive functionality. Although PCs abound in the enterprise landscape, they are no longer the only devices for delivering services and applications to users.

Tablets are fulfilling the role of the primary device for an increasing group of users. For example educational institutions are moving toward making tablets the primary systems for students, and verticals such as retail, healthcare, legal, real estate, media and others are embracing tablets as well.

Until now, the dominant tablet product in the industry has been the iPad, but with Windows 8, Microsoft Corp. is hoping to unsettle the trend. The Microsoft Surface tablet showcases both flavors of Windows 8 – Windows 8 Pro (powered by x86 processors) and Windows RT (powered by ARM processors).

With so many tablets running so many operating systems, IT organizations will need to determine how they are going to manage these new technologies that enable their enterprise's flexibility and user choice, while helping maintain security.

2.3 Persistent growth of Mac and Linux

Those "other" operating systems in the enterprise, Macintosh and the various flavors of Linux, aren't out of the OS race yet; in fact they're gaining momentum. Red Hat, Ubuntu and SuSE Linux are growing share among corporate users, partly for servers, and Apple keeps growing Macintosh customer base inside the enterprise space (5% by 2015 per Gartner).[3] According to a June 2012 report from Forrester Research, 37% of information workers were using non-Windows devices for work in 2011.[4]

These slow but steady increases only serve to broaden the variety in enterprise IT environments.

2.4 Consumerization of IT

Hardly an employer in America has not grappled with employees using personal devices, laptops and others, to do company work. This "bring your own device" (BYOD) practice has gradually been sanctioned by IT organizations despite security, compliance and liability concerns. Consumerization of IT is not simply a passing trend, so IT managers must respond with policies to support these devices and to secure any intellectual property or corporate data they contain.

[3] "Forecast: PC Market by Operating System, Worldwide, 2011 Update," Gartner Inc., July 1, 2011, ID:G00214411.
[4] "Charting The Rising Tide Of Bring-Your-Own-Technology," Forrester Research, by Connie Moore, June 12, 2012, http://www.forrester.com/Charting+The+Rising+Tide+Of+BringYourOwn+Technology/fulltext/-/E-RES72366

2.5 Complexity, not homogeneity

In a 2011 survey of IT professionals[5], 69% said that employees bring desktops and laptops running Windows, Macintosh and Linux to work. The survey, conducted by Dimensional Research for Dell KACE, also found that 62% of IT professionals expressed concerns about network security because of personal devices; they also said that they lacked the tools necessary to manage them.

This proliferation of devices and platforms in the enterprise has vastly complicated the work of IT administrators who must efficiently and scalably support multiple devices and operating systems without compromising corporate security policies. If someone in the C-suite wants an iPad, even if it's not an approved device, IT must figure out how to provide support. The homogeneous IT environment, if it ever existed as much in reality as in belief, has evaporated as employee choice has become enshrined in the name of employee productivity. Not supporting the iPhone is no longer an option in many companies because executives and employees alike see it as a necessary tool.

2.6 Endpoint security

Keeping the many new devices and their software secure is a vexing issue for IT managers. Data breaches reached an all-time high of 174 million records in 2011, 98% from external sources including cybercriminals and hacktivists.[6] The variety of applications and operating systems in the corporate environment has significantly increased the complexity for IT organizations that now have to make sure that security-enhanced solutions are in place for all the different types of systems. Also with so many devices and operating systems and the foray of personal devices in the work place, a hacker seeking access to a corporate network needs only to crack one of the many devices that access corporate data.

3.0 Best Practices

1. **Automate operations/Hold down headcount.** To counteract rising IT personnel costs from supporting corporate users and systems, turn to automation. One-time costs to buy technology that automates IT tasks across multiple operating systems is cheaper than hiring new people for each new operating system. As a bonus, automating system management can free IT workers to address more strategic corporate objectives.

   Each enterprise's systems management needs will vary, but key priorities for automation include imaging and re-imaging machines, patching, backups, asset management, configuration and policy management, security audit and enforcement, service desk, remote software installation and distribution, managing remote sites and remote PC users, and inventory of all devices on the network.

   Savvy IT leaders will future-proof systems management with a solution that supports new operating systems. Also, be sure the inventory function finds not only devices with supported operating systems but also identifies and reports on devices running

[5] https://www.kace.com/resource-center/resources/Consumerization-of-IT-Survey-2011

[6] "Data Breach Investigation Report," Verizon, 2012, http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

unsupported ones. Knowing what's on the network is the first step to managing those devices in a secure and scalable way.

2. **Invest in multi-platform tools—a no-brainer.** Buy standards-based IT infrastructure tools that support multiple platforms in a consistent and scalable way. Single-platform tools may offer great solutions for a specific platform, but they are dead ends if they must be replaced or ported in the heterogeneous IT environment. A web-based tool, unlike a platform-specific mobile app or a Windows graphical user interface, can extend to multiple platforms and devices. Of course, for some tasks, only proprietary or platform-specific tools are available, so sometimes IT shops will be forced to go that direction.

3. **Keep IT tools updated.** Keeping IT tools updated is critical to be able to stay ahead of the technology curve on devices and operating systems. This means any solution that IT uses should provide regular updates to reflect latest technological changes. And more importantly, the upgrade process should be simple and non-disruptive. Given the rate of technology change, it would be impractical to have to invest in forklift upgrades for each new version to gain its improvements. As technology advances, ensure that upgrading to newer versions of software is as simple as possible. Pay attention to vendor roadmaps, and tell your vendor what's still missing in its products. Vendors may listen or they may already have decided to support specific technologies, devices or software. If you really need something, ask for it; you may get it addressed sooner, not later. Pick management tools that plan to support the latest operating systems as they are announced.

4. **Know thy network.** A bullet-proof inventory system lets you know what's on your network, the first step to securing your network, applications and data. The ability to detect, inventory and asset manage all devices on the corporate network is critical to corporate security. Any application that is not corporate approved can potentially open a security backdoor into the corporate network. Don't settle for a less-than-complete inventory tool that can't tell you about everything on your network.

5. **Secure endpoints.** The deluge of new devices and software has IT organizations struggling to keep endpoints protected. Running multiple operating systems on a network opens multiple targets for security attacks thereby increasing the risk of breaches. Securing endpoints in such a diverse environment requires multiple implementations of security measures for each and every platform in the corporate network. A solution that enables IT to implement security policies in a consistent way across all the different operating systems is recommended.

   That means utilizing a "layered security" approach that uses multiple levels of security enhancements to keep endpoints safe, including automated patching and incorporated leading security technologies such as encryption, anti-virus software, firewalls, virtual private networks (VPNs), etc. Consider single-sign-on (SSO) or other technologies to ease (and thus secure) how users access applications on all their devices. For companies subject to regulatory requirements, security issues quickly become compliance issues, so managing everything on the network is paramount.

4.0 The Case for Dell KACE to Manage Multiple Operating Systems

The Dell KACE K1000 Management Appliance allows IT to manage both corporate-issued and personal devices on multiple operating systems including Windows, Mac OS X and Linux. The KACE K1000 Appliance helps simplify IT management by automating management of more devices with the same (or fewer) people. Among its features:

"I used to spend up to two days a month managing software updates for Windows, but with the Dell KACE K1000 I'm monitoring both Windows and Macs, but I've reduced the time I spend on updates to half a day per month." -Mikko Kauttu, CIO, Optinet

- Automated IT administration: The K1000 automates the routine tasks required to manage endpoints and helps ensure security and compliance. IT tasks can be scheduled easily and can be targeted at specific systems through the label feature. As multiple operating systems in the IT environment increase the complexity for IT, the ease-of-use, automation and intuitive user interface of the K1000 helps IT cut complexity and improve efficiency.
- Support for multiple Operating systems: Supports Windows, Mac and Linux[7] platforms for both clients and servers which offers a consistent management solution[8] for laptops, desktops, tablets and servers.
- Inventory management and device discovery: Knowing what is in the corporate network is the first step toward implementing an effective system management infrastructure. The K1000 supports popular operating systems and also has a machine inventory API that allows it to extend inventory capabilities to operating systems that are not supported by the K1000 agent. With the K1000 IT organizations can view, track, report on and asset manage all laptops, desktops, servers and tablets from a single web-based console.
- Web-based user interface and email ticket creation: The K1000's management console utilizes industry standards to make it easy for IT to support a heterogeneous multi-platform environment. It uses a familiar browser-based interface that is available from any Web-enabled device so sys admins don't need to learn a whole new management console on a proprietary platform. Users can easily create tickets either through the user-portal or by simply sending an email to the K1000 service desks. This ensures that all users are supported regardless of platform or device.
- Ease of upgrades: Unlike competing systems management packages, K1000 upgrades are a matter of clicking a button, not requiring new software or hardware installations and avoids the need to invest in expensive resources to accomplish manual and complex upgrade processes. In addition, the K1000 automates agent updates to the K1000 server thereby simplifying the process of keeping endpoints up-to-date.

[7] The full list of operating systems support in the K1000 includes Windows 8 x86 (Professional, Enterprise), Windows 7 (Professional, Enterprise, Ultimate), Windows Vista (Business, Enterprise, Ultimate), Windows XP (Professional), Windows Server 2012 (Foundation, Essentials, Standard, Data Center), Windows Server 2008 R2 (Enterprise, Standard, Web), Windows Server 2008 (Enterprise, Standard, Web), Windows Server 2003 (Enterprise, Standard, Web), Mac OS X 10.4 - 10.8 PowerPC and x86 architectures, Linux Red Hat Linux AS and ES Versions 3, 4, 5 and 6, 64-bit architecture, Ubuntu Linux Versions 10.x, 12.x, SuSE Linux Enterprise Server Versions 11.x

[8] Patching not available for Linux.

- Endpoint security: The K1000 delivers robust endpoint security capabilities (and security enforcement) by complementing traditional security software such as firewalls, creating an integrated, layered approach to security and systems management. The K1000 inventories devices on the network, automates configuration and patch management, handles software distribution, identifies and remediates vulnerabilities across end nodes, manages and enforces compliance with company policies for desktops, laptops and servers, and quarantines compromised systems to help prevent them from infecting the rest of the network. Its security audit and enforcement capabilities include pre-built security policy settings and robust reporting for regulatory compliance and other purposes. By integrating with other technologies such as data encryption, firewalls, anti-virus software and VPNs, the K1000 becomes part of a layered security solution that increases network security.
- User Portal: The K1000 user portal offers users a self-service option to accomplish many routine support tasks like downloading approved software, creating service desk tickets and checking ticket status. It also allows users to share best practices and collaboratively rank usefulness of various training and support resources. In a heterogeneous environment with multiple operating systems, devices, and applications, the user portal improves IT efficiency by significantly cutting down support calls thereby allowing IT to focus on more strategic projects.

5.0 Conclusion

The proliferation of operating systems and devices threatens to choke IT department, bust IT budgets and burn human resources that could better be spent on higher corporate priorities.

With the growing diversity of desktop, laptop, tablets and mobile devices, enterprise IT departments are finding manual management has become too complex and costly. IT executives should look for automated, easy-to-use tools to simplify device management and implement best practices of the heterogeneous endpoints on their networks.

About The Author

Tim Clark is a senior analyst and partner at The FactPoint Group in Silicon Valley. His specialties include network security, appliances, Software as a Service, data center management software, open source and virtualization. He was previously a senior analyst at Jupiter Research and VP/senior analyst at Net Market Makers. Previously, Tim was a journalist for 24 years, working as senior editor and columnist for CNET's News.com, where his coverage areas included Internet security. He has written multiple white papers for Dell KACE.

www.factpoint.com

Dell KACE Corporate Background

Dell (NASDAQ: DELL) creates, enhances and integrates technology and services customers count on to provide them reliable, long term value. Dell provides systems management solutions for customers of all sizes and system complexity. The award-winning Dell KACE family of appliances delivers easy-to-use, comprehensive, and affordable systems management capabilities.

Dell KACE is headquartered in Mountain View, California. To learn more about Dell KACE and its product offerings, please visit www.dell.com/kace or call 1-877-MGMT-DONE.

Helpful Links:

- **KACE Systems Management Appliances**
- **KACE Systems Deployment Appliances**

Dell KACE Headquarters
2001 Landings Drive
Mountain View, California 94043

(877) MGMT-DONE office for all inquiries
(+1) (650) 316-1050 International
(650) 649-1806 fax
kaceinfo@dell.com
European Sales: kaceemea@dell.com
Asia Pacific Sales: kaceapac@dell.com
Australia New Zealand Sales: kaceanz@dell.com
Greater China Sales: kacegc@dell.com

WPMultiOS08.31.2012