Enabling safe and secure BYOD in the enterprise with Dell KACE K Series Management Appliances

Eric Liefeld
Katavolt Media
# Table of Contents

1.0 Introduction .......................................................................................................................... 3
2.0 Responding to BYOD challenges.......................................................................................... 3
   2.1 Enabling BYOD in the face of rampant device proliferation ............................................. 3
   2.2 Providing mobile data security .......................................................................................... 4
   2.3 Managing the risk of growing complexity ........................................................................... 4
3.0 Dell KACE: A holistic and effective approach to BYOD ....................................................... 4
4.0 Embracing BYOD with Dell KACE Appliances .................................................................... 5
   4.1 Managing personal devices ............................................................................................... 7
   4.2 Managing personal laptops and tablets running Microsoft Windows, Mac OS X, and Linux ............................................................................................................................. 7
   4.3 Managing mobile Apple iOS and Google Android devices ................................................... 8
5.0 Conclusion ............................................................................................................................. 8
Dell KACE Corporate Background ............................................................................................... 9
1.0 Introduction

For many, work is no longer seen as a place, but as an activity that is independent of both location and specific technology. With that independence comes increasing diversity in the types of devices used for communication and productivity, and new challenges in terms of managing both personal and corporate applications and data. From laptops to smartphones and tablets, mobile devices in particular contribute a compelling computing model that can bring real benefit to a wide range of organizations. Being able to access corporate content on personal devices allows employees to work anytime from anywhere, and improves productivity and flexibility. Many of these devices now integrate enterprise capabilities such as e-mail and calendaring, making them vital tools for the people who use them.

As a result of this shift, organizations are moving from being PC-centric to a user-centric model, where employees bring their own devices (BYOD) and choose those devices that best suit their specific needs at any particular time or circumstance. While these trends have great benefit for employee productivity, they are bringing significant challenges, since IT staff no longer has complete control over what devices and operating systems can be used in a corporate setting. In fact, while Gartner now estimates that 90% of organizations will support corporate applications on personal devices by 2014, they also note that 100% of IT organizations are struggling to keep up with mobility trends¹. In a recent survey of 750 IT professionals by Dimensional Research, 80% reported that employees used smart phones, and 87% said that employees used personal devices for work². A majority of those surveyed also expressed concerns about network security breaches due to the use of these personal devices, and also said that they lacked the tools necessary to manage them.

2.0 Responding to BYOD challenges

In formulating effective BYOD strategies, organizations must grapple with a range of challenges to accentuate the positive attributes of new technology without compromising the needs of the organization.

2.1 Enabling BYOD in the face of rampant device proliferation

The development lifecycle for mobile devices is extremely short, and new devices and different form factors arrive constantly. Employees now view their use of these devices as a basic need, and organizations are embracing smart phones and tablets as attractive application deployment platforms. For example, educational, healthcare, and other institutions are moving rapidly toward making tablets the primary system for information disbursement, because of the convenience of an easily portable form factor coupled with robust functionality. Other industries such as retail, legal, real estate, media, and marketing are embracing tablets and smart phones as well.

IT organizations must move rapidly to safely and securely support as many devices as possible. Managing tablets and smart phones requires different approaches from managing desktop computers, but the high-level requirements of security and policy enforcement are the same. In order to be “enablers” of BYOD capabilities, IT organizations must stay ahead of the curve in adopting and

---

¹ [http://www.gartner.com/it/page.jsp?id=1480514](http://www.gartner.com/it/page.jsp?id=1480514)
² [http://www.techjournal.org/tag/dimensional-research/](http://www.techjournal.org/tag/dimensional-research/)
permitting new technologies. Ignoring trends and industry best practices will not only hurt IT, but can compromise the effectiveness of the entire organization.

2.2 Providing mobile data security
Security for corporate data is typically the biggest concern for the IT organization. While mobile devices have long been a part of the corporate environment, IT organizations have managed these devices with varying levels of control. Unfortunately, mobile devices are at a higher risk of falling into the wrong hands, so the ability to secure sensitive data is essential. If an employee loses a mobile phone, IT needs to be able to lock out any access to corporate content from the lost device. Likewise, when an employee leaves the organization, IT needs to be able to cleanly remove all corporate content from their mobile devices. This ability is important both to protect corporate content, and also to maintain employee privacy.

2.3 Managing the risk of growing complexity
Gone are the days when IT departments had full control over the choice of device and operating system, with the luxury of supporting a fairly homogeneous environment. Increasing complexity means risk for IT administrators, and securing corporate content on personal devices is critical. A hacker only needs to break into one of the many mobile devices that access corporate data to gain entry into the company’s network. Unfortunately, the proliferation of devices and operating systems dramatically increases the complexity for IT, and also increases the risk of security attacks.

IT organizations are struggling with quickly adopting new technology changes to ensure that mobile endpoints continue to stay protected. Complicating matters, employees now have an average of three-to-four devices, generating a nightmare for the organizations that must support them all. A user self-help program is absolutely essential to be able to support personal devices as part of an effective BYOD program.

3.0 Dell KACE™: A holistic and effective approach to BYOD

Beyond merely supporting myriad new devices, IT departments must enable secure access to sensitive corporate information on an ever-changing range of consumer-grade mobile phones, laptops and tablets. Effective safeguards must be provided for valuable corporate data and applications, since regulatory compliance ultimately depends on having control over all of the devices on corporate networks. At the same time, even as users seek access to corporate content, their own privacy rights must be strictly respected. Balancing these needs requires a holistic approach to BYOD management.

Unlike standalone management platforms, the Dell KACE approach considers mobile device management as a simple extension to desktop, laptop, and server management. Dell KACE K Series Appliances help IT organizations move quickly from merely coping with multiple disparate devices to enabling comprehensive, safe and secure BYOD activities within their organizations, by providing:

- **A single solution for all devices.** Having a single management solution for all devices results in a true user-centric experience.
- **Unified trouble ticketing.** The KACE Service Desk can handle trouble tickets for all of a user’s devices—indeedent of type—greatly simplifying the experience.

---

3 Dell Consumerization Research, September 2011
- **Asset reporting.** Having consolidated inventory and asset management reports for all devices greatly simplifies management tasks for IT.
- **Consistent application of IT policies.** With KACE K Series Appliances, IT policies can be applied consistently across all devices.

## 4.0 Embracing BYOD with Dell KACE Appliances

Dell KACE K Series Appliances enable IT organizations to embrace BYOD by securely supporting the popular personal devices that employees bring to work. With the family of Dell KACE K Series Appliances, IT professionals can provision, deploy, manage and report on all supported personal devices. This comprehensive, integrated, and easy-to-use solution lets organizations manage desktops, laptops, servers, and mobile devices throughout the organization, and allows personal devices to safely and securely access corporate content, regardless of platform, ownership, or form factor. Dell KACE K Series Appliances also help IT organizations solve the challenges posed by the proliferation of devices and operating systems, allowing organizations to secure, track, update and manage across a broad range of diverse personal devices (Figure 1).

![System Lifecycle Management](chart.png)

Figure 1. Dell KACE K Series Appliances allow organizations to embrace BYOD across diverse mobile systems and operating systems.

The Dell KACE Family of Systems Management Appliances is designed to help save time and money by providing end-to-end Microsoft Windows, Mac OS X, Linux and virtual machine systems management capabilities, as well as support for mobile operating systems such Apple® iOS and Google Android™. All appliances support plug and play deployment onto corporate LANs and are simple to upgrade and
maintain. Virtually no upfront programming is required to enable the appliances. Dell KACE Appliances are also available as both physical and virtual appliances, providing a range of cost-effective deployment options. Together these appliances offer:

- Comprehensive systems management functionality including core mobile device management (MDM) features
- Ease of use with quick and automated deployment and maintenance, and monitoring and management through an intuitive Web-based user interface (Figure 2)
- Affordability through appliance-based delivery

![Figure 2. Dell KACE Appliances provide monitoring and management through an easy-to-use Web-based interface.](image)

Dell KACE K Series Appliances are designed to work together to deliver a fully integrated systems management solution, unlike traditional software approaches that can require complex and time-consuming deployment and maintenance. Dell KACE provides an extremely flexible and intelligent appliance-based architecture that typically deploys in days, and is self-maintaining. Appliances in the K Series family include:

- **Dell KACE K1000 Management Appliance**. The Dell KACE K1000 Management Appliance is a fully integrated systems management solution for Microsoft Windows, Mac OS X® and Linux operating systems.
• **Dell KACE K2000 Deployment Appliance.** The Dell KACE K2000 Deployment Appliance automates the provisioning of Microsoft Windows and Mac OS X based systems.

• **Dell KACE K3000 Mobile Management Appliance.** The Dell KACE K3000 Mobile Management Appliance integrates with other K Series Appliances to detect, track and control both Apple iOS and Google Android personal devices in a corporate setting.

### 4.1 Managing personal devices

Though they are used for work-related tasks, personal devices need to be managed differently from corporate owned devices, since they are employee owned, and contain private data. Moreover, with each user typically accessing corporate data with multiple devices, handling support and self-service proactively is critical to avoid rapidly over-burdening IT staff.

• **Corporate data, personal privacy.** While IT departments exercise complete control over corporate owned devices, only corporate content should be secured on personal devices, without compromising employee privacy. Dell KACE Appliances allow IT departments to easily group personal devices for policy application. KACE Appliances also allow IT to create policies to specify personal vs. corporate content.

• **Personal vs. corporate devices.** The Dell KACE labeling feature lets IT departments group personal devices using labels, and apply configuration and security settings for personal devices that are different from corporate devices—allowing for scalable management.

• **Self-service.** Dell KACE Appliances offer a self-service user portal designed to enable users to support their own personal devices, lessening the burden on support staff. Users can track their devices, see an inventory, download approved applications and software, and collaboratively share guidelines and best practices.

• **Rapid provisioning.** Dell KACE Appliances automate and simplify the provisioning process for personal devices on all popular platforms. Employees can have their personal devices provisioned for corporate access in a matter of minutes.

Dell KACE Appliances also offer software distribution for applications on personal devices along with remote management, patching, configuration management, security, service desk, reporting, and other functionality.

### 4.2 Managing personal laptops and tablets running Microsoft Windows, Mac OS X, and Linux

The Dell KACE K1000 System Management Appliance lays the foundation for BYOD by helping IT departments manage personal laptops on Microsoft Windows, Mac OS X, and Linux platforms. Laptops can be provisioned for corporate access, discovered, tracked and managed for compliance with IT security policies. Separate configurations can be created for personal devices, specifying approved software that can be downloaded onto those devices, what settings should apply, and which security criteria need to be met.

The Dell KACE K1000 Management Appliance offers IT staff a wide range of functionality, and the flexibility to help BYOD activities align with company-specific security policies. Different processes can be created for managing personal devices versus corporate owned devices. For example, while corporate-owned devices are typically patched automatically, notifications can be sent to personal devices, informing of available patches. Corporate access can be made conditional on patch compliance to limit security exposure. This functionality removes the burden from IT staff by significantly reducing support calls for personal devices.
4.3 Managing mobile Apple iOS and Google Android devices

The Dell KACE K3000 Mobile Management Appliance allows IT departments to support personal devices that run Apple iOS or Google Android—comprising approximately 82% of the mobile OS marketplace as of this writing. The appliance dramatically simplifies complex mobile-specific provisioning tasks into one single step through a secure setup process. Over-the-air provisioning of agents to mobile devices gets them up and running quickly on corporate networks.

The appliance extends system management capabilities to enforce security policies for mobile devices. Mobile device data security capabilities protect corporate data on mobile devices through profile management, device lock and unlock, remote enterprise wipe, and remote factory reset features. The appliance can also enforce and manage configurations to implement corporate IT policies, and allows creating and managing device, application, and user-based profiles on all managed devices. The self-help user portal allows users to enroll their personal devices for corporate access, and they can push approved applications to their personal devices without calling the support desk. This ability allows IT departments to roll out BYOD programs quickly and in a scalable fashion.

The application deployment and management feature allows IT departments to push approved corporate applications to personal devices and also to track and monitor usage. The profile management feature allows IT staff to track devices for compliance with security policies, send notices to users in the case of non-compliance, and revoke access to corporate content if violations persist. When an employee leaves or wishes to relinquish corporate access, the enterprise wipe feature allows for removing corporate content, while leaving personal content untouched.

5.0 Conclusion

As work patterns shift from an in-office desktop-based model to an anytime, anywhere, any device model, IT organizations need to move quickly to provide safe and secure BYOD solutions. Mobile devices are entering the market every day in a range of form factors, presenting new opportunities for employees to be effective, agile and productive. Representing more than just a risk or an annoyance for IT departments, support for BYOD is now a corporate imperative. Organizations need to be able to seamlessly grant secure access to essential corporate applications and data to provide workplace flexibility and employee productivity, without compromising end-user privacy.

The Dell KACE K Series Appliances help IT departments manage and enforce security policies on personal devices that access corporate content, from Microsoft Windows and Mac OS X-based laptops to Apple iOS and Google Android-based smart phones and tablets. As a fully integrated solution that is easy to use for both employees and IT managers, Dell KACE K Series Appliances offer a comprehensive solution for managing supported desktops, laptops, servers, and mobile devices, making secure BYOD an achievable reality for the organization.

For more information, please visit:

http://www.kace.com/solutions/byod

---

Forecast: Mobile Devices by Open Operating System, Worldwide, 2009-2016, 2Q12 Update
About the Author
Eric Liefeld is a senior writer with Katavolt Media. His specialties include network and data center architecture, virtualization and cloud computing, technical and high-performance computing, and graphics and visualization, among other technical topics. Eric has been involved with data center technology for 30 years, with background and experience in systems administration, systems engineering, and technical communications. He has written multiple white papers for Dell KACE.

http://www.katavoltmedia.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

WPBYOD11.30.2012
While every effort is made to ensure the information given is accurate, Dell does not accept liability for any errors or mistakes which may arise. Specifications and other information in this document may be subject to change without notice.