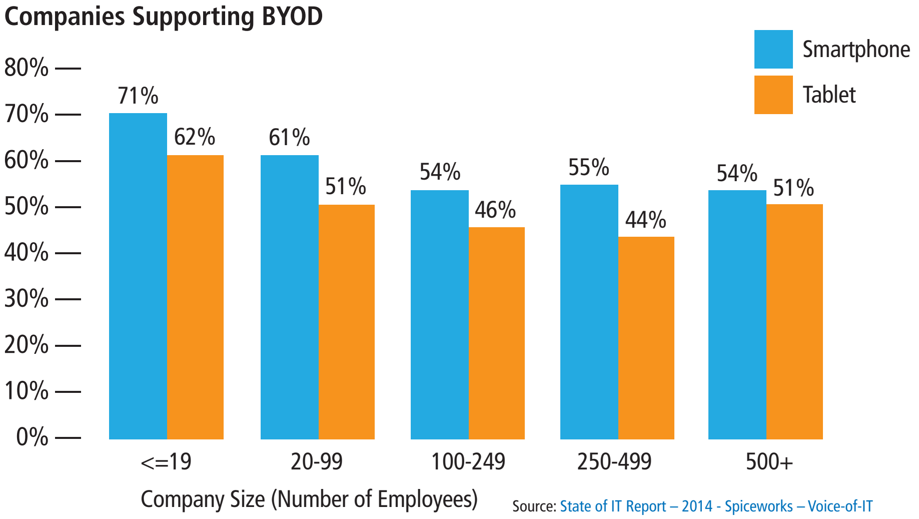
Kaseya® White Paper

A Smarter Approach to Secure BYOD Management

Kaseya®

THE IT MANAGEMENT CLOUD COMPANY™

Mobile devices have become a preferred means of accessing data and applications, wherever and whenever individuals desire. On average, individuals have two to three devices that they use today. Employees expect to use their own preferred tools and technologies to do their work, and their personal mobile devices are chief among them. The BYOD (Bring Your Own Device) trend, therefore, is now mainstream and growing rapidly in acceptance. Forrester estimates that 70% of mobile professionals will conduct their work on personal smart devices by 2018. Businesses big and small are supporting BYOD today, as seen below in a survey of 1000+ IT professionals.



Source: State of IT Report – 2014 - Spiceworks – Voice-of-IT

> “By completely isolating personal assets from enterprise assets and the network, containerization keeps the personal device “personal,” and free to be used for non-enterprise purposes.”

What are the Challenges of BYOD Management?

BYOD presents significant challenges for IT management around security and employee satisfaction and acceptance. They include:

- **The Risk and Manageability Challenge**
  Personal devices in the workplace bring a new set of challenges, such as:
  - How can organizations set up and manage access on employees’ mobile devices?
  - What happens when a device is lost or stolen?
  - Can the organization ensure that company data is wiped from the phone and access to enterprise systems is immediately shut off if needed?

  A heavy-handed approach to managing mobile devices, in which the organization controls all data on that device, was the widely accepted approach used when mobile devices were typically provided by the organization. While this approach meets organizations’ needs for data security, in a BYOD environment employees will not allow this sort of draconian control over their personal devices.

  A new solution is needed for BYOD management in which company data can be secured without invasive levels of control and oversight over employees’ personal data and activities on their devices.

- **The Employee Satisfaction and Acceptance Challenge**
  People tend to develop strong attachments to the devices they carry for their personal communication needs. The reality is that if businesses don’t give employees the ability to work with the tools they want to, in the ways they want to, employees will go outside of the company standard and bring their own tools and technologies into the equation anyway. This rogue,

unmanaged scenario poses tremendous risks to enterprise data security, not to mention creating employee dissatisfaction. Furthermore, employees also are often strongly averse to the inconvenience of carrying a second, "non-personal" mobile device, often of a different type and operating system, to perform essentially the same function for professional purposes.

Businesses on the other hand also benefit from this trend of employees seeking to achieve work-life integration on a single device, without compromising their privacy. A mobile management solution that addresses BYOD challenges must satisfy the needs of both IT professionals and the mobile users they serve.

The question thus becomes, how can organizations not just enable mobility and BYOD, but embrace it in ways that drive employee engagement and productivity, without incurring risks to organizational data security? The challenge for organizations is not to prevent BYOD, but rather to find new ways of meeting enterprise requirements that are appropriate for this new environment.

The Solution: Containerization as Winning Strategy for BYOD Management

The solution to this BYOD dilemma – balancing the needs of the enterprise with the demands of its users – is "containerization" technology on mobile devices. With installable apps that create isolated 'containers' on an employee's personal device, organizations can provide a secure environment controllable by the organization.

Unlike MDM (Mobile Device Management) solutions, which control the entire mobile device and all of its contents, containerization is uniquely suited to BYOD management because it segregates company and personal data on the device.

Containerization gives IT the tools it needs to establish separate, encrypted, policy-enforced "containers" within personal devices, and to deliver email, browser apps, and data specifically to those containers. Policy and management extend only to the container's contents, which reside in complete isolation from the rest of the device. Company data within these containers is encrypted at rest and in flight, and isolated from the rest of the data and apps on the device. If a device is lost or stolen, IT can wipe the containers without disturbing personal assets. There is no enterprise need for users to set device level security, as only their personal data is at risk should they choose to leave their devices unprotected.

To further protect the enterprise, communications with containers can be conducted over a private communications channel that encrypts and authenticates each connection, eliminating the need for VPNs or other inbound TCP/IP connections from the device to the enterprise network. This approach shields the network from probes, attacks, malware, and compromised devices, as only the secure containers connect to the enterprise network.

By completely isolating personal assets from enterprise assets and the network, containerization keeps the personal device "personal," and free to be used for non-enterprise purposes. Users are able to use the devices they carry at all times for convenient and secure enterprise access, with that access as familiar as all other device use.

Given the arrival of such technologies that enable secure enterprise access from personal devices, it was inevitable that BYOD management would become an integral component of mobile strategies across companies.

BYOD Management Solutions as IT Relief

BYOD management is often seen by IT as a challenge in which it must balance the need for protection against data theft and unauthorized access with users' needs for personal-device flexibility and freedom of use. Traditionally it's far more orderly and efficient for IT departments to set standards for the hardware and software it is responsible for supporting instead of users selecting their own hardware and OS as their end points.

BYOD by nature breaks that model, requiring a higher level of flexibility with users and a new

> **"The ability of BYOD management and MDM to coexist relieves IT from the burden of having to manage every mobile device used for enterprise access, and relieves users from being subject to a one-size-fits-all approach to mobility management."**

management paradigm for new challenges. Unlike desktop/laptop computing, the smartphone and tablet markets offer a rapidly growing number of devices and OS variety, which is very acute with the Android platform.

But when IT is no longer responsible for managing the device, there are significant advantages for both enterprise IT and end users. Given a safe and secure access methodology, IT should be no more obligated to support a personal smart device than it is obligated to support users' home computers. Users in turn gain the ability to share information and access enterprise resources on the device they've already mastered for personal use.

Without the requirement to manage the device and OS – and with the right BYOD platform delivering an innovative approach to secure mobile access – IT can be freed to focus on the core issue at hand i.e. securing information assets and protecting enterprise resources.

Co-existence of Containerization and MDM

Containerization may not solve every enterprise need for every mobile user, and containers and MDM (Mobile Device Management) needn't be viewed as mutually exclusive. In many deployments, the two methodologies may be mixed and matched according to mobility roles.

For employees who need routine access to shared documents, Intranet sites, and HTML or hybrid apps, containerization is typically sufficient to enable productive mobility that is both secure and convenient. Eliminating MDM and enterprise-owned devices for these employees can also significantly reduce enterprise costs while giving users the satisfaction of flexibility. Containerization further extends meaningful, controlled access to partners and customers for whom MDM is simply not viable.

Other roles may warrant MDM. That's especially the case when the job function is completely mobile or requires information access beyond email/PIM, documents, and intranet apps. In such cases, it may be simpler to supply enterprise-owned devices completely managed by IT. Even then, the use of containers within the enterprise-owned device can add an additional layer of security and application management. It is more common to have a single employee use a company-owned device, as well as personal device, to access company data, documents and intranet apps. For this, the solution needs to provide the agility to IT admins to apply BYOD management or MDM controls to devices selectively without breaking the bank.

The ability of BYOD management and MDM to coexist relieves IT from the burden of having to manage every mobile device used for enterprise access, and relieves users from being subject to a one-size-fits-all approach to mobility management. As long as employees are informed as to the reasons they're getting containers or MDM on their devices, and how these measures protect both employee and enterprise, the result will likely be a much more satisfied, mobile-empowered workforce.

Putting Containerization to Work for You

BYOD management is rapidly becoming a fact of life. Thanks to the introduction of new technologies that make it practical, workable, and secure, the BYOD dilemma – balancing the needs of the enterprise with the demands of its users – has been greatly diminished. Now is the time to consider containerization as the means to increasing mobile productivity and improving collaboration, while controlling costs and keeping IT focused on managing applications rather than devices.

> “Thanks to the introduction of new technologies that make it practical, workable, and secure, the BYOD dilemma – balancing the needs of the enterprise with the demands of its users – has been greatly diminished.”

About Kaseya

Kaseya is the leading provider of cloud-based IT management software. Kaseya solutions allow Managed Service Providers (MSPs) and IT organizations to efficiently manage IT in order to drive IT service and business success. Offered as both an industry-leading cloud solution and on-premise software, Kaseya solutions empower MSPs and mid-sized enterprises to command all of IT centrally, manage remote and distributed environments with ease, and automate across IT management functions. Kaseya solutions are in use by more than 10,000 customers worldwide in a wide variety of industries, including retail, manufacturing, healthcare, education, government, media, technology, finance, and more. Kaseya is privately held with a presence in over 20 countries. To learn more, please visit **www.kaseya.com**

Kaseya®
THE IT MANAGEMENT CLOUD COMPANY™