WHITE PAPER:
EXPLOITING THE BUSINESS POTENTIAL OF BYOD

Exploiting the business potential of BYOD (bring your own device)

Who should read this paper

This paper addresses the challenges of BYOD and is relevant for anyone looking into providing a corporate policy allowing employees to bring their own devices of choice.

Content

Executive Summary

The way we do business is changing. The trend for employees to use personal mobile devices at work is on the increase. Organisations have to weigh up the productivity benefits this brings against the major security challenges it incurs. This paper will consider the implications of mobile computing within the workplace and look at how implementing the right strategy, developing the right policies and choosing the right solutions can help an organisation leverage BYOD potential while protecting valuable business assets. Key content will include an overview of the benefits of Mobile Device Management (MDM) and Mobile Application Management (MAM) solutions and how these can be combined. The paper will also discuss the importance of including all mobile devices, including laptops and notebooks, within any strategic plan.

Introduction

Just as the Internet has changed the way we do business, mobile devices are quickly becoming a similar catalyst. Once deemed off-limits by businesses, smartphones are now being used by hundreds of millions of employees to access corporate data. Tablets are also increasingly being used for both work and leisure activities, with mobile functionality a key driver.

In fact, a recent Symantec survey[1] showed we have reached a tipping point in the business use of mobile devices as mainstream business activity. The report found companies were embracing this change: nearly three quarters of the organisations surveyed were looking to develop their own customer mobile applications, well over half were running line-of-business applications, and two-thirds were discussing implementing a corporate 'app store'.

So why has the use of personal devices as business tools changed from a largely forbidden activity to an acceptable practice? The answer lies in today's emphasis on business agility. Mobile devices are helping companies to increase workforce effectiveness, increase efficiency, and generally get work done more quickly. Adding something around potential for new business as customers and partners are equally becoming more mobile.

Enterprise mobility delivers on productivity because employees know how to use, and enjoy using, their own devices. BYOD can also reduce capital expenditure as businesses can leverage devices employees may already be paying for. In addition, employees often take better care of devices they have selected and purchased.

However, the rise of BYOD culture also brings its own problems for businesses; it can increase productivity but can leave an organisation with a risk assessment nightmare. A 2011 Gartner report stated that: "Although BYO is attractive to some enterprises, it poses a range of new challenges for the support organisation. No organisation can afford to fix an unlimited range of issues on a large portfolio of devices, many of which the organisation doesn't own and therefore can't control in conventional ways."

"No organisation can afford to fix an unlimited range of issues on a large portfolio of devices, many of which the organisation doesn't own and therefore can't control in conventional ways."

Gartner, July 2011

Organisations are aware of the potential dangers mobility can pose, rating it highest among IT initiatives in risk. They're worried about losing devices, data loss and malware infecting the corporate network through smartphones and tablets. And there is good reason for these concerns. Businesses are losing a significant amount of money to incidents relating to mobile devices; as much as USD$429,000

1-Symantec, State of Mobility Survey, 2012

annually in the case of large enterprises[2]. Despite these costs, however, organisations feel the risks are worth the benefits, and are working to implement security measures to keep corporate information safe.

In this paper, we will review the challenges around BYOD and consider the best practices a business can undertake to leverage its potential while safeguarding valuable business assets.

BYOD Challenges

Understanding user behaviour and demands

Although many organisations are committed to corporate mobile computing, this does not always apply to individual employees. An IT Policy Compliance Group report[3] found that the business risks are purposely restricting the number of employees using mobile devices within the workplace. Although 79% of organisations surveyed used smartphones to access information and applications at work on a corporate level, the number of actual employees using smartphones for this purpose was just 33%. Similarly, while 35% of companies surveyed used tablet computers for corporate purposes, the average number of their employees using tablet computers was just 22%.

Mobile computing can save costs, but without policing it could prove costly. Although potential savings can be made from employees bringing their own devices, firm control of costs related to data roaming and traffic is vital. As employees turn more and more to mobile subscription plans paid for by the employer, traffic charges can increase unless price plans and policies (such as imposing WiFi usage) are introduced to avoid hefty mobile bills.

Corporate nervousness about mobile computing is understandable. Most of today's mobile devices operate in an eco-system outside of the enterprise's control. Many employees synchronise their devices with at least one public cloud-based service as well as home computers. This can leave sensitive data stored in insecure locations; not to mention the risks associated with corporate e-mail being sent through personal accounts such as Gmail™, or file-sharing services such as Dropbox.

However, despite the risks, there is no doubt that employees are increasingly using their personal devices to improve their productivity at work. So it makes sense for companies to manage these risks and make this trend work for them, rather than against them.

Defining a strategy

The first step for an organisation is to develop a mobile strategy which clearly defines what its objectives will be. Many organisations do not consider what they would like to achieve with BYOD: for example, whether it's to promote increased efficiency, generate greater productivity or drive actual revenue growth.

Developing the right policy

To implement a mobile policy, an organisation needs to understand where business information is stored, how it is accessed and by whom.

A company should address the following four 'A's in its policy:

- **Assess**: threats, conduct a risk analysis, run a policy audit and an apps audit, evaluate architectural planning and security.
- **Accommodate:** policy updates, device management, private apps store, content repository, secure iPads®/tablets, data loss prevention, authentication, encryption, CSP mobile security and basic app access.
- **Access:** to mobile enterprise app enablement (MEAP) and mobile development, operational streamlining, service provider intelligence and information access.

2-Best Practices for Supporting 'Bring Your Own' Mobile Devices , Gartner, July 2011
3-Managing the Benefits and Risks of Mobile Computing, IT Policy Compliance Group, 2011

- **Advantage:** to be gained across vertical applications, mobile business process outsourcing (BPO), mobile e-commerce, and social and mobile integration.

Integrating management

Mobile devices can be viewed as just another endpoint, so it makes sense to integrate them into existing systems' management. In addition, because laptops, mobile devices and desktops all need management, configuration and policies, implementing separate point solutions just adds to IT complexity.

Integrating mobile management into existing management solutions, such as Altiris™ Client Management Suite from Symantec or Microsoft® System Center Configuration Manager, help reduce costs, improve efficiency, and lower total cost of ownership.

Implementing best practice

Any mobile strategy should take into consideration the following best practice recommendations:

- **Enable broadly.** To get the most from mobile advances, plan for line-of-business mobile applications that have mainstream use. Employees will use mobile devices for business one way or another – make it on your terms. Set clear and measurable objectives for productivity gain, employee satisfaction and customer services.
- **Think strategically**. Build a realistic assessment of the ultimate scale of your mobile business plan and its impact on your infrastructure. Think beyond e-mail. Explore all of the mobile opportunities that can be introduced and understand the risks and threats that need to be mitigated. As you plan, take a cross-functional approach to securing sensitive data. Ensure your mobile strategy is future-proof and accounts for rapid changes in usage, increasing number of devices and emerging platforms.
- **Manage efficiently**. Mobile devices are legitimate endpoints that require the same attention as traditional PCs. Many of the processes, policies, education and technologies that are leveraged for desktops and laptops are also applicable to mobile platforms. So, the management of mobile devices should be integrated into the overall IT management framework and administered in the same way – ideally using compatible solutions and unified policies. This creates operational efficiencies and lowers the total cost of ownership.
- **Enforce appropriately**. As more employees connect personal devices to the corporate network, organisations need to modify acceptable usage policies to accommodate both corporate-owned and personally-owned devices. Management and security levers will need to differ based on ownership of the device and the associated controls that the organisation requires. Employees will continue to add devices to the corporate network so organisations must plan for this legally, operationally and culturally.
- **Secure comprehensively**. Look beyond basic password, wipe and application blocking policies. Focus on the information and where it is viewed, transmitted and stored. Integrating with existing data loss prevention, encryption and authentication policies will ensure consistent corporate and regulatory compliance.
- **Consider the cloud**. Not only will employees expect to access cloud services from mobile devices, but be aware that the success of the mobile world is dependent on cloud services to store and access information.

It is also worth noting that the principles of a mobile computing strategy are equally relevant for employees who bring their laptop of choice to work.

Solutions to support BYOD

There are many solutions available and considerations should include whether managed or unmanaged services are needed, the separation of corporate and personal information required and the impact of cloud services.

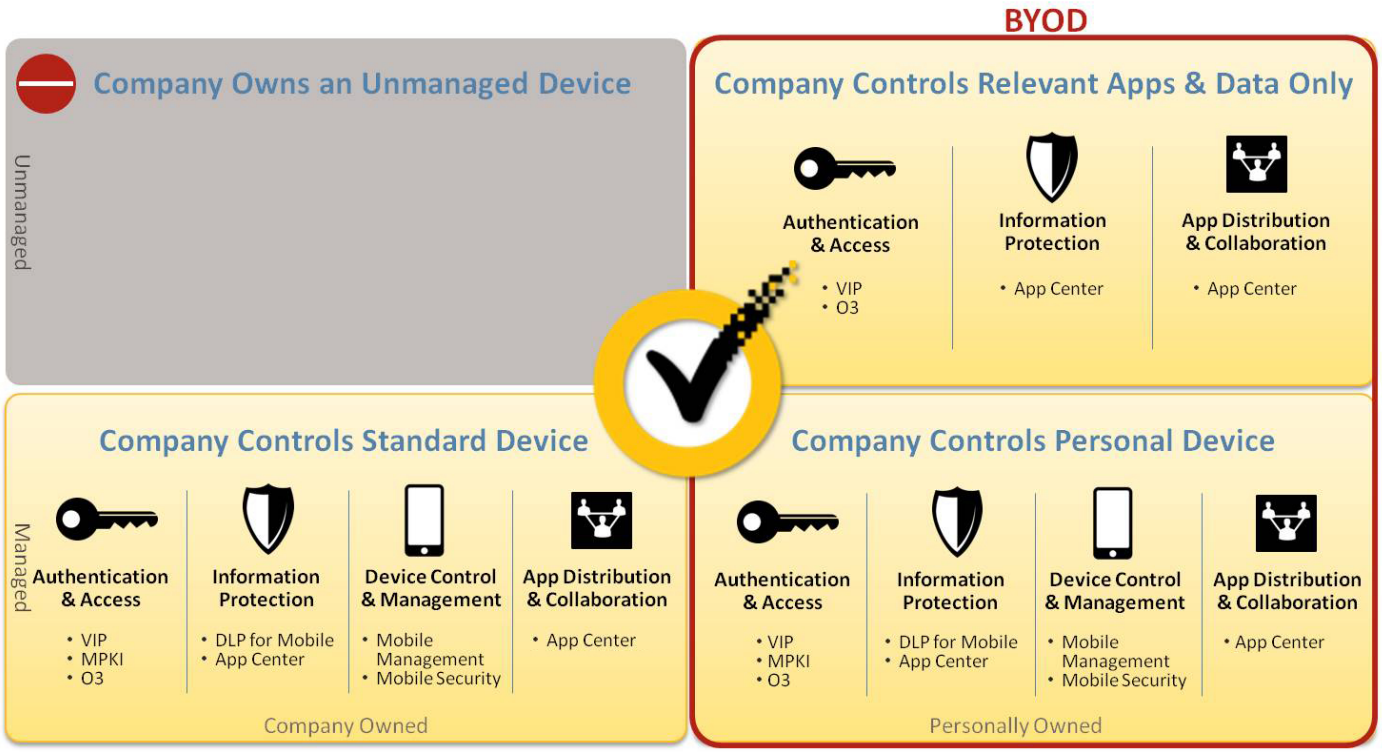

Figure 1: Bring your own device matrix

Mobile Device Management (MDM)

This solution enables the remote administration and enrolment of managed mobile devices. Typical security policies might include setting password strength, configuring VPN settings, specifying screen lock duration and disabling specific app functions (such as access to App stores) to prohibit potentially risky behaviour. In addition, administrators can perform security operations such as locating or wiping lost or stolen devices.

Mobile device management solutions don't specifically protect against any risk category. However, the ability to remotely configure the device, for example to block all new apps, can help eliminate the introduction of malware and also limit resource abuse, integrity threats and intentional (or unintentional) data loss.

Separation of personal and corporate data can also be achieved with an agent based mobile device management solution as the removal of the agent itself will only affect corporate data and applications.

Mobile device management is typically considered by organisations in need of a comprehensive mobile solution that incorporates a corporate app store and shared document libraries. It allows for a broader approach to productivity than merely providing access to email and calendar, which is the most common level of mobile access today.

Mobile Application Management (MAM)

Mobile application management is becoming an increasingly relevant alternative or complement to mobile device management. It refers to software and services that accelerate and simplify the creation of internally developed corporate mobile applications.

This approach views the applications and the related information and services supplied by smartphones and tablet computers as the vital part of the infrastructure, rather than the devices themselves. For organisations, a corporate app store is the key tool to providing secure and correct access to corporate mobile apps. It enables companies to define policies for the application (who should have access and on what level, from what device should access be granted, and how can the information retrieved through the app be utilised) rather than the device.

Unlike mobile device management, which requires remote management to be granted by the employee who might be reluctant to provide access to some functions and settings, mobile application management targets only the applications accessing corporate data.

App distribution functionality also enables organisations to leverage third party or custom applications, which is becoming a key business driver to add value and generate competitive advantage.

Combining MDM and MAM

Depending upon business objectives, many organisations will need to combine the two above mentioned solutions. While some functions need to take advantage of the full range of enterprise mobility or deal with sensitive information that will require managed solutions, others might suffice with access to a selected number of applications. The imperatives an organisation set will decide whether it should opt for a fully-fledged management solution for all mobile employees or a hybrid version where employees/functions are classified based on department objectives and needs.

Don't forget the laptops

The fact that not only smartphones and tablets should be considered as mobile devices, but also laptops and notebooks, adds another dimension to an organisation's mobile strategy concerns. In many instances, preferred laptops of choice will be brought into the corporate network and will be subject to either a managed (as discussed previously) or an unmanaged scenario. Common instances of this could include educational institutions or service branches, where employees need access to a number of applications to be able to perform their jobs.

Endpoint virtualisation and workspace streaming allow end users to instantly acquire applications as needed on desktops, laptops, VDI, Terminal service and Citrix, according to authorisations and productivity needs. Minimal bandwidth is required since applications can function with only a small percentage delivered, and streaming is self-service, so IT staff do not need to be notified or involved.

Cost-effective management is the main benefit. Delivery of applications is based upon need and will help reduce license costs and improve management as applications can easily be upgraded and controlled.

Symantec solutions

Symantec offers a wide choice of mobile computing product solutions designed to support businesses in their strategic objectives.

Mobile Device Management

Symantec™ Mobile Management

Delivers over-the-air deployment of applications and updates, device health monitoring and complete lifecycle management of mobile devices to increase IT efficiency and user productivity. Symantec Mobile Management integrates with Microsoft System Center Configuration manager and Altiris Client Management.

Mobile Application Management

Symantec App Center

Provides secure Mobile Application Management (MAM) capabilities for native mobile apps. MAM products are used to manage the growing needs of enterprises to manage and secure mobile applications, particularly in BYOD environments.

Information Protection when mobile

Symantec Mobile Security

Advanced device security including reputation based security for Android™ and Windows® Phone. Symantec Mobile Security will be available later this year.

Symantec™ Data Loss Prevention for Mobile

Monitors and protects sensitive data sent from iPad and iPhone® mail clients, browsers, and apps, such as Facebook, Twitter and Dropbox. Unlike other solutions that restrict users from accessing apps and files on their iPads and iPhones, Data Loss Prevention for Mobile enables secure use of sensitive data without stopping business.

Symantec Verisign Identity Protection (VIP) Access for Mobile

Verifies user identity by generating a unique security code or one time password and turns a mobile phone into a strong two-factor authentication security device, eliminating the need for additional security hardware.

Symantec™ Managed PKI

Cloud-based service to power strong authentication, encryption, and digital signing of applications.

Symantec PGP Mobile

Comprehensive email and data encryption solution for Windows Mobile smartphones and data cards.

Symantec PGP iOS viewer

Decrypts encrypted email attachments on iOS devices directly and enrols them for key management.

Collaboration and Cloud/Mobile access

Symantec O_3

Cloud security platform designed to protect all enterprise cloud applications and cloud infrastructures. O_3 works across public, private, and hybrid clouds to manage access control and protect information as it flows between enterprise applications and users and the various cloud services they rely on every day.

Summary and next steps

The intent of this paper is to provide guidance around BYOD and present solutions and strategies to take the next steps. Below some useful links are presented to provide additional information and tools to enable the next steps towards enterprise mobility.

Take the Mobile health check to evaluate your mobile risk level: https://www.emea.symantec.com/mobilehealthcheck/
Symantec Mobile pages: http://www.symantec.com/en/uk/mobile-device-security

Was this paper useful to you? Please let us know by participating in the discussion on https://www-secure.symantec.com/connect/blogs/byod-challenges-and-opportunities.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Symantec helps organizations secure and manage their information-driven world with **data deduplication** and **deployment software**.

7/2012 21256109-1