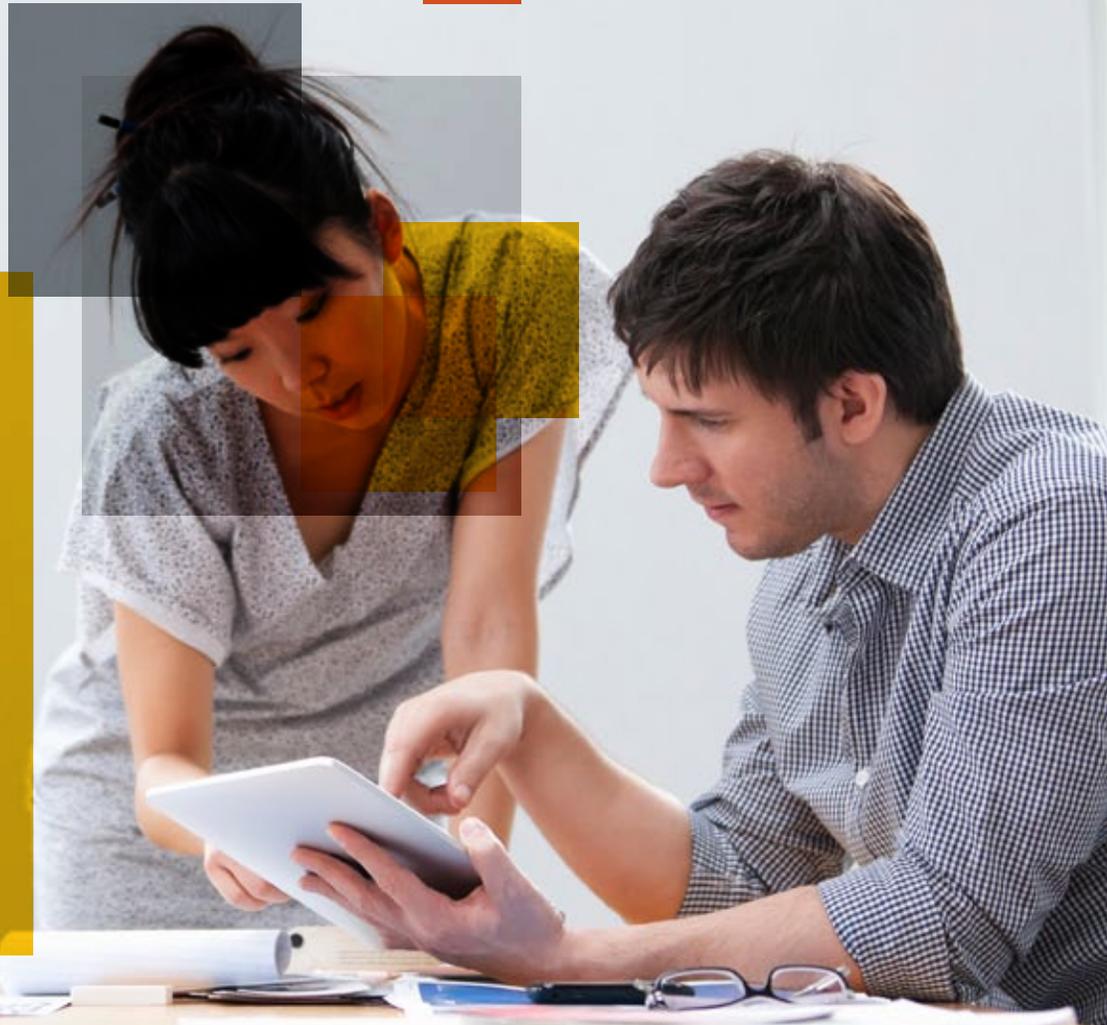


# ENTERPRISE MOBILITY:

Enabling Productivity without  
Sacrificing Protection

Confidence in a connected world.



## BYOD AND OTHER MOBILE CHALLENGES

### Employees are using mobile devices for business—whether you like it or not.

Companies often recognize the opportunities of mobility—the ability to do things they could not do before, creating new business opportunities and competitive advantages. But most businesses also see mobility as a challenge. More people are working outside of the firewall than ever before, in multiple locations, at flexible times, and on a number of different devices. This phenomenon started years ago on traditional laptops and later Macs, but today’s challenge is multiplied many times over with the introduction and tremendous popularity of smartphones and tablets. Moreover, many users are insisting on using personally owned devices, giving rise to the massive BYOD (Bring Your Own Device) movement. Now, IT organizations must not only deal with remote connections and personal devices, but also new operating systems and an unprecedented diversity of hardware.

#### There are at least two reasons to pay attention to this trend:

1. Many companies are finding increased end-user productivity when mobile devices are enabled for business use. There are often competitive advantages for companies that leverage line-of-business and custom apps on mobile devices.
2. Employees are using mobile devices for business, whether it is sanctioned or not. The methods they use are often in conflict with company policies and government or industry regulations, and the potential risk to company data when employees are working around the system can be enormous. It is generally far better (and safer) to have a strategy that allows controlled mobile access than to have no strategy at all.

So how can IT effectively enable mobility without exposing their companies to the risks inherent to business computing on personal devices and unmanaged networks? First, recognize that business mobility necessarily implies that people are working outside of the traditional PC-centric model that has evolved in IT over the last 20 years or so, and people behave differently in this more flexible and open environment. People buy their own devices and their own applications (apps); they log on to their devices differently; they communicate freely across managed and unmanaged networks; they leverage cloud services almost constantly; and most importantly, they blur the lines between business and personal.

Enterprise IT feels the impact. Today, 65% of surveyed companies allow employees to access the network with their own devices; 52% of these workers regularly use three or more devices. Further, 80% of newly developed applications are not based on-premise, but deployed in the cloud.

- Symantec, “State of Mobility Report”  
February 2012

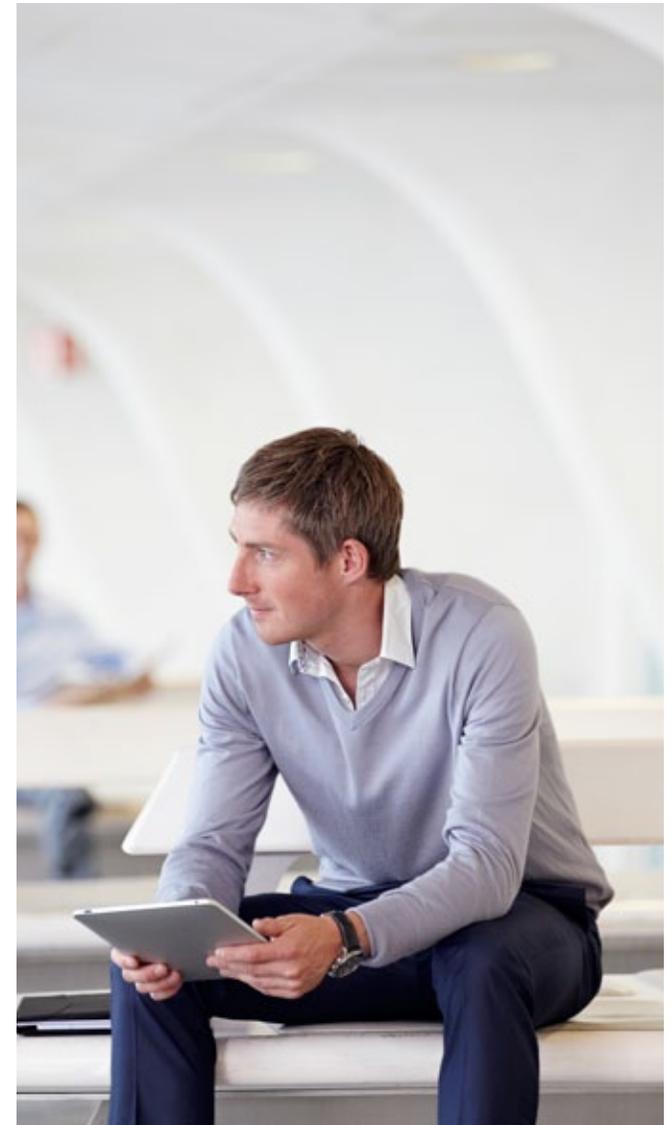
## The Total Mobile Solution

### Productivity *and* protection are only accomplished with a comprehensive solution

In the early days of mobility (up to about 2 years ago), devices were mostly owned by businesses and used primarily for communications (phone and email). Shortly after the introduction of smartphones and tablets, mobile device management (MDM) software appeared to help manage and configure these devices, in a similar fashion to PCs. As individuals have increasingly gone mobile for business productivity, leveraging apps to access, store, and transmit more corporate data, businesses must realize that the challenge is now bigger and MDM is insufficient on its own for all but the very simplest of use cases. The challenge is now about enabling, securing, and managing devices, apps, and data that reside outside the firewall or in the cloud, requiring a more comprehensive approach to business mobility.

**With these diverse challenges, there are five key areas that every company must consider as they establish their mobile strategies to ensure high productivity without increasing their vulnerability. These five pillars of enterprise mobility are as follows:**

- 1. User and App Access:** People, the apps, and the devices that are connecting to, and accessing, business assets must be identified and validated as authorized business participants. Identity is the first and most important component to any IT strategy, especially where mobility is involved, due to the frequent use of cloud apps and access from multiple devices, where identity is often more difficult to determine.
- 2. App and Data Protection:** Business data must be protected at all times. Mobile apps are the primary method to access, view, store, and transmit that data, and with more apps in use, there is more sensitive data on mobile devices. Direct control of specific, critical apps and data (as opposed to device-based control) is a very effective approach to apply the desired layers of protection exactly where they are needed, without touching the remainder of the device. This is a critical component for BYOD.





3. **Device Management:** Devices that access business assets and connect to company networks must be managed and secured according to applicable company policies and industry regulations. Every company should establish appropriate mobile policies, and those should be applied to all managed devices, just as policies and configurations are applied to corporate PCs and laptops.
4. **Threat Protection:** With the incredible growth of mobile devices in the world, they are rapidly becoming the new preferred target for bad guys. Different platforms have different risk profiles, and it is important to understand where vulnerabilities exist and to take appropriate action to secure business assets. Good threat protection should protect from external attacks, rogue apps, unsafe browsing, theft, and even poor battery use.
5. **Secure File Sharing:** Although access, storage, and sharing of files are not uniquely mobile challenges, multiple device ownership and the need to collaborate make the cloud a driver for productivity, allowing for simple distribution and synchronizing of information across devices. Businesses should have full administrative control over distribution of, and access to, business documents on any network, especially in the cloud.

Each of these five pillars represents a category of technologies that may stand on its own. In fact, there are companies that have built businesses entirely around each individual pillar. However, for mobile environments, these functions are very interrelated, and the common mobile use cases require companies to implement a combination of pillars. In most cases, all five pillars must be represented to achieve acceptable levels of productivity and protection across the business. Ideally, the pillars would not be just represented, but there should also be numerous points of integration among pillars to enhance protection, productivity, and even IT efficiency and cost. This highly desirable integration can only be accomplished by a single company offering solutions in all five pillars, as Symantec does.

	 <b>USER &amp; APP ACCESS</b>	 <b>APP &amp; DATA PROTECTION</b>	 <b>DEVICE MANAGEMENT</b>	 <b>THREAT PROTECTION</b>	 <b>SECURE FILE SHARING</b>
<b>Primary Products</b>	Symantec O <sub>3</sub>	App Center	Mobile Management	Mobile Security	Content Center
<b>Complementary Products</b>	Managed PKI Service Validation and ID Protection	DLP for Mobile PGP Encryption	IT Management Suite Client Management Suite	Endpoint Protection	O <sub>3</sub>

## Which Symantec Products Support Each Pillar?

### User and App Access

- Symantec O<sub>3</sub><sup>™</sup>
- Symantec<sup>™</sup> Managed PKI Service
- Symantec<sup>™</sup> Validation and ID Protection

### App and Data Protection

- Symantec<sup>™</sup> App Center
- Symantec<sup>™</sup> Data Loss Prevention for Mobile
- Symantec<sup>™</sup> Mobile Encryption for iOS
- Symantec PGP<sup>™</sup> Viewer for Android

### Device Management

- Symantec<sup>™</sup> Mobile Management
- Symantec<sup>™</sup> Mobile Management for Configuration Manager
- Symantec<sup>™</sup> Client Management Suite
- Symantec<sup>™</sup> IT Management Suite

### Threat Protection

- Symantec<sup>™</sup> Mobile Security
- Symantec<sup>™</sup> Endpoint Protection

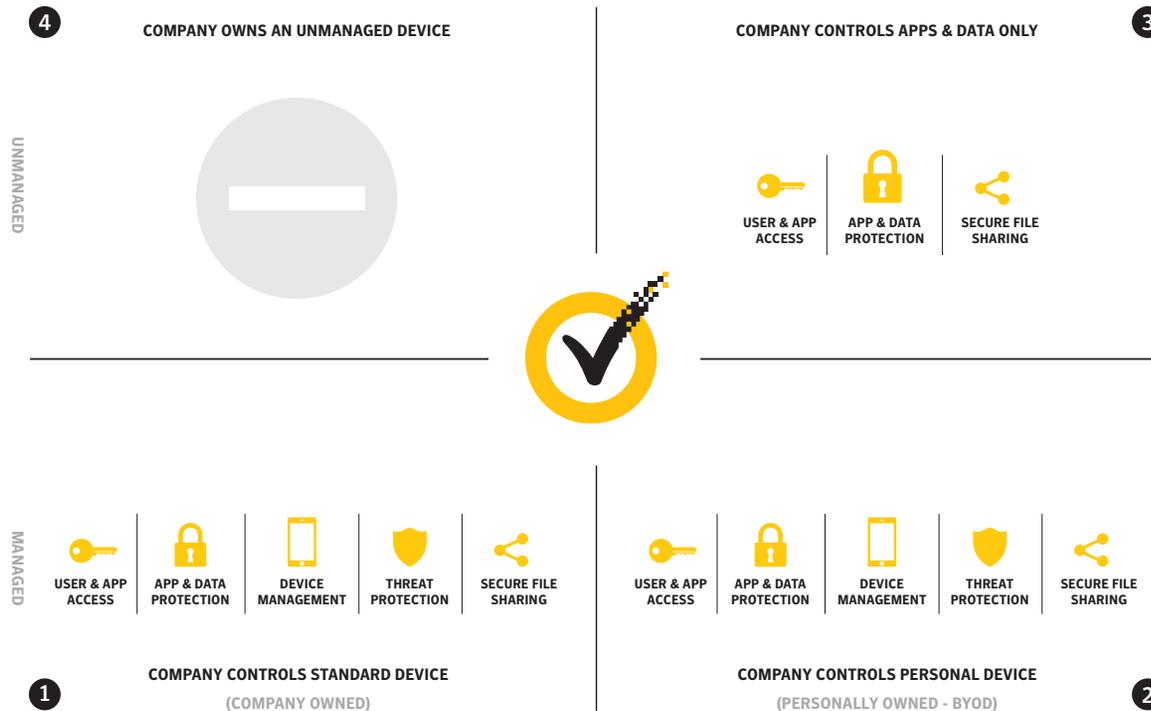
### Secure File Sharing

- Symantec App Center
- Symantec O<sub>3</sub>

## Mapping mobile adoption

### A Journey with Multiple Destinations

Every company will have a different path to mobile adoption, and final implementations will vary, depending on the needs of various business functions and on regulations that impact mobile policies. A simple way to evaluate where a business is and where it wants to be is to look at devices in terms of who owns them and to what degree they are managed. The result is the 2X2 matrix shown, which identifies the four different environments where one might find devices of any kind in business.



Note that there are two approaches for the BYOD scenario. On the bottom, the same approach may be applied as in Quadrant 1 by managing the device as a whole. While above, in Quadrant 3, that luxury does not exist and IT must put more emphasis on individual applications to accomplish the desired protection and control. An easy way to differentiate these approaches is to refer to them as device-centric and app-centric.

- 1 The lower left quadrant** is the most familiar, representing the traditional approach to IT. The company provides standard equipment to its employees from a limited set of configurations, and it installs agents for full control over configuration, management, and security. For mobile devices, this is really no different than for traditional PCs and laptops—if the device is owned, it should be managed.
- 2 In the lower right**, corporate control must be identical to the first quadrant because the requirement to protect data and networks does not change with personal ownership of the device. There is, however, a big difference in liability and expectation of privacy. As long as the controls and limitations imposed on the device are not too severe, this can be a good model for both the business and the user. For industries that are more heavily regulated, like healthcare, finance, and government, the required controls and policies will be more limiting and not as reasonable for a user who has purchased their own device (see Quadrant 3).
- 3 In the upper right**, there is no attempt to apply policies or controls over the entire device, as in the lower half. Instead, it recognizes that the information that needs to be protected will generally be accessed and contained within specific applications. Therefore, if there is a way to apply safeguards around the applications in question, there may not be a need to apply controls over the entire device. This approach works well for organizations that want to move to a user-owned model, yet regulations and necessary policies prevent the full control approach from being practical.
- 4 The upper left** is an undesirable place to be, where the company owns the device, yet it has no control (and often no visibility) over them. This frequently happens when an executive uses company money to buy a mobile device and then proceeds to use it for business without informing IT. Devices that are in this quadrant should be moved into one of the other quadrants as quickly as possible, typically by adding a management agent and moving it down to Quadrant 1.

## How to Proceed

### Individual Strategies for Individual Businesses and Departments

Every company, and even departments within companies, will have a different path to mobile adoption, and final implementations will vary significantly. It is important to understand which issues must be addressed in each quadrant to ensure both productivity and the protection of critical information. [Note that the five pillars discussed previously have been overlaid on the quadrants to indicate which are applicable and should be included in the strategy for those devices.] With the opportunity, and desire, for so many businesses to move to a BYOD model, this chart makes it clear that there are two distinct approaches to BYOD—device-centric and app-centric. The device-centric model in the lower right really only works for relatively simple cases where the controls are not too severe for the owner and the business risk tolerance is relatively high or access is limited. The app-centric model in the upper right is fast becoming a popular destination because business data may be locked down very tightly, without touching personal apps or impacting the end-user experience.

For every situation, there are essential tools to manage devices, protect information, and assure productivity. At Symantec, we continue to build on the broadest, most comprehensive solutions for enterprise mobility to ensure each company, and each unique need within a company, may be optimally addressed and satisfied.



**Your employees are moving to mobile devices.**

**Are you ready to move with them?**

It's not a question of whether you want your employees conducting business through mobile devices, but whether you want visibility and control over mobile activity they are already engaged in—activity that can have significant consequences for your business.

**Is your enterprise ready? Test yourself against this brief checklist:**

- Are employees productive with devices they already know, use, and understand?
- Can you secure company data without compromising users' personal data and privacy?
- Can you apply protection policies directly to critical apps and data on unmanaged devices?
- Do you know who is accessing enterprise assets and resources, regardless of location and/or device?
- Can you maintain visibility and control of employee business activity on public clouds?
- Can you ensure a consistent standard of control, regardless of the type and number of devices?
- Are you as protected against mobile malware threats as you are against attacks against PCs?
- Can employees securely synchronize, share, and collaborate over the cloud?
- Do you have consistent security policies and procedures for company-owned and employee-owned devices?
- Can you manage effective access, encryption, and authentication controls on specific applications?
- Are you able to scale your policies to any number of devices of any kind?

If you're not confident that you can answer "yes" to all these questions, it may be time to obtain greater confidence in your controls. Talk to a Symantec enterprise security partner by calling 1-888-252-5551 or writing to [AltirisSalesInfo@symantec.com](mailto:AltirisSalesInfo@symantec.com). Or learn more about Symantec and mobile trends by visiting us online at <http://go.symantec.com/mobility/>.

**For more information**

Visit our website

<http://go.symantec.com/mobility>

**To speak with a Product Specialist in the U.S.**

For details on product coverage for your area, call toll-free +1 (888) 252-5551 or visit <http://go.symantec.com/mobility>

**To speak with a Product Specialist outside the U.S.**

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

**About Symantec**

Symantec protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment—from the smallest mobile device to the enterprise data center to cloud-based systems. Our industry-leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at [www.symantec.com](http://www.symantec.com) or by connecting with Symantec at [go.symantec.com/socialmedia](http://go.symantec.com/socialmedia).

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](http://www.symantec.com)

Confidence in a connected world.

