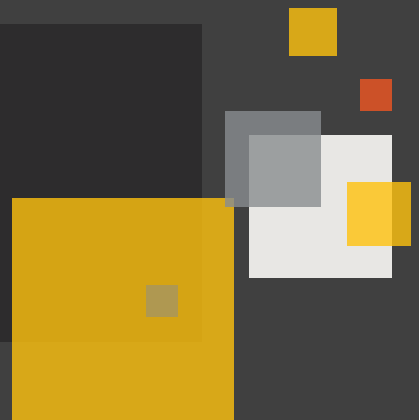




# ENTERPRISE MOBILITY USE CASES AND SOLUTIONS



# ENTERPRISE MOBILITY USE CASES AND SOLUTIONS

Mobility is no longer a trend – it's how business gets done. With employees using multiple mobile devices and the availability of thousands of mobile apps, employees can work whenever and wherever they choose. This also means IT now has the dual challenge of supporting mobile productivity and protecting corporate data.

Symantec's mobility solutions have been designed to help organizations address this challenge. By managing apps and devices using granular, policy-based controls and deploying market-leading mobile threat protection, you can proactively enable mobile productivity without compromising security. Here we explore the strategic use cases that Symantec's mobility solutions can help with.

**USE CASE 1**  
**Mobilize Business Processes**



[LEARN MORE](#)

**USE CASE 2**  
**Distribute Apps and Content**




[LEARN MORE](#)

**USE CASE 3**  
**Allow Access to Only The Right People**




[LEARN MORE](#)

**USE CASE 4**  
**Prevent Mobile Data Leaks**



[LEARN MORE](#)

**USE CASE 5**  
**Offer Secure Alternatives to Consumer Apps**




[LEARN MORE](#)

**USE CASE 6**  
**Block Malicious Mobile Threats**



[LEARN MORE](#)

**USE CASE 7**  
**Support BYOD and CYOD**



[LEARN MORE](#)



## USE CASE 1:

### MOBILIZE BUSINESS PROCESSES

Organizations view mobility as game-changing technology that can streamline business processes, improve customer service and satisfaction and enhance employee productivity. These organizations are looking to provide relevant and secure mobile apps, either custom-developed or commercially off-the-shelf to employees, contractors, and partners.



### CSU, NETHERLANDS

“Our vision for mobility is to introduce a solution that provides users with a seamless experience for interacting with enterprise data, without compromising either productivity or privacy. In addition to offering that technology vision, Symantec addresses CSU’s key goals for securing its mobile workforce: user access, data protection, device management, and threat protection.”



### IT CHALLENGE:

- How do I deliver and secure mobile apps that my line-of-business peers are demanding?
- How do I support strategic initiatives to improve highly manual, time and labor intensive processes using mobile apps?
- How do I enable line-of-business projects when IT is brought in at the tail end of a project?

### SOLUTION:

Symantec Mobility Suite helps secure mobile apps using granular, policy-based controls applied on an app-by-app basis. Policies are dynamically applied without developer resources or the need to reinstall apps. The Symantec Sealed Program provides a trusted ecosystem of commercially off-the-shelf apps that can be managed via Symantec Mobility Suite.

### HOW SYMANTEC MOBILITY SOLUTIONS CAN HELP:

- Mobilize key business processes by securing and distributing content such as sales catalogs, training manuals and medical information to mobile devices.
- Secure and distribute apps, independent of how the apps are developed (native, hybrid, Web, or HTML5) allowing developers to choose the development method that best achieves the desired outcome.
- Deploy, secure, and manage mobile apps and content on corporate-owned and employee-owned devices.
- Wrap a layer of security controls around mobile apps without delaying project rollout. Customers have been able to wrap apps in 5-10 minutes without developer resources.
- Deliver secure collaboration apps such as Secure Email and Secure Web along with Symantec Sealed versions of many third-party apps. These apps deliver a consumer-like experience with enterprise-grade security to protect data in-transit and at-rest.

## USE CASE 2: PROVIDE A SECURE WAY TO SHARE APPS AND CONTENT

With so many apps available today, IT needs a user-friendly way for employees, contractors and partners to get the apps and content they need to get their job done.



### MUNICIPALITY OF HERNING

“The best feature from Symantec is the built-in app store, which enables us to customize the distribution of applications to our staff. We can simply target a given application at a given staff group and secure that only that group has access.”



### IT CHALLENGE:

- How do I provide an easy way for employees, contractors, and partners to get the apps and content they need to get their job done?
- How do I deliver a secure and user-friendly mobile workspace to employees, contractors, and partners?
- How do I provide a secure alternative to consumer-grade apps my users are already using to review and edit documents, take notes, instant message, chat and text with co-workers?

### SOLUTION:

Symantec Mobility Suite lets IT set up a branded enterprise app store allowing for easy distribution of custom apps, third-party apps, and enterprise content to authorized users. Providing an enterprise app store not only makes it easy for employees, contractors, and partners to get the apps they need but it also helps deter them from downloading potentially dangerous (and unsanctioned) apps to their devices.

### HOW SYMANTEC MOBILITY SOLUTIONS CAN HELP:

- Deploy an enterprise app store that allows for easy distribution of custom-developed apps, third-party apps, and content to employees or other authorized users, such as contractors or partners.
- Ensure apps are deployed to appropriate users by targeting apps for specific groups. Users can view and access only the apps and content they are allowed to use, based upon their role.
- Gain insights from user ratings, comments, and reports that allow you to make better decisions regarding developing new apps, enhancing, maintaining or retiring the existing apps.
- Speed mobile productivity with an ecosystem of trusted and secure third-party mobile apps from the Symantec Sealed Market Place.



### USE CASE 3:

#### ALLOW ACCESS TO ONLY THE RIGHT PEOPLE

There is no question that mobile devices have become an integral part of today's workplace. Many organizations realize that enabling a mobile workforce means they need to provide more widespread access (for example, to partners), to protect their user and device identities from compromise, and to ensure that mobile activities do not impact or jeopardize privacy and regulatory requirements.



#### LARGE HEALTHCARE INSTITUTION IN SOUTH AMERICA

“To enable faster access to patient information and improve an already high standard of care, we needed a solution that would track and manage mobile devices and apps, and provide seamless, secure access to the hospital network for our doctors and healthcare professionals. Symantec gives us a single integrated solution for mobile device and certificate management. As a result, caregivers get patient information in minutes rather than hours and we're saving a lot of time.”



#### IT CHALLENGE:

- How do I provide the right level of access to data on mobile devices to the right people?
- How do I protect my mobile users beyond user names and passwords even if I have an MDM solution in place?

#### SOLUTION:

Symantec Managed PKI Service (MPKI) and Symantec Mobility Suite deliver and manage user certificates that enable seamless access to Wi-Fi, VPN, and Exchange ActiveSync. With Symantec Mobility Suite, IT has the ability to validate users, devices, and apps that are accessing the network. Symantec gives organizations peace of mind that sensitive data is protected on mobile devices.

#### HOW SYMANTEC MOBILITY SOLUTIONS CAN HELP:

- Provide convenient, secure, cloud-based two-factor user authentication and public key infrastructure (PKI) services for protecting users accessing accounts from any device.
- Verify the identity of the individual, validate the device, and secure the transportation of information to guard against any unauthorized access with Symantec's digital certificates. Symantec also supports integration with Microsoft CA.
- Control mobile access to corporate resources such as VPN, Wi-Fi, and Exchange ActiveSync with integration of Symantec MPKI and Mobility Suite.
- Simplify certificate management with Symantec MPKI mobile-aware certificates.
- Extend identity and authentication with SAML integration; simplifies user experience with one username and password.

## USE CASE 4: PREVENT MOBILE DATA LEAKS

Protecting corporate data in today's mobile environment is a significant challenge for IT. Mobility introduces new risks in the enterprise such as employees adopting unapproved mobile or cloud-based apps for work, corporate data leaking into unmanaged mobile or cloud-based apps, unauthorized access to corporate data, and lost or stolen devices.



### QUEST DIAGNOSTICS

“In the mobile examiner space, we were using a costly paper-based process for people to go out and take blood draws remotely. We needed to get a tablet solution to capture that data electronically and send it securely to the lab to ensure PHI and HIPPA compliance. With the Symantec mobility solution, we saw an increased lab result turn-around time with great data protection.”



### IT CHALLENGE:

- How do I prevent data from intentionally or accidentally leaking to unauthorized mobile apps and/or the cloud from mobile devices?
- How do I ensure that corporate data on mobile devices is secured in the event it gets compromised?

### SOLUTION:

Symantec Mobility Suite addresses these challenges with integrated MDM, MAM, and Threat Protection capabilities. For example, Symantec's device management (MDM) allows you to prevent non-compliant devices from connecting to corporate assets. Symantec's application management (MAM) protects corporate apps and data through a unique technology that wraps a layer of security and policy management around mobile apps. Symantec's Threat Protection provides powerful, effective protection against unauthorized access to sensitive corporate information.

### HOW SYMANTEC MOBILITY SOLUTIONS CAN HELP:

- Symantec Mobility Suite's data protection policies allow IT to control the flow of data between apps. IT can specify what apps a document can be opened in and whether content can be copy/paste from one app to another. Policies can be applied on a per-app basis.
- Symantec offers advanced security solutions to protect access from unauthorized users by enabling device, app, data and network policies (e.g. device wipe, jailbreak detection, Wi-Fi and VPN), encryption, multi-factor authentication, certificate management, data loss prevention and network protection via secure gateways.
- Mobile apps in the Symantec Sealed Program have been wrapped with a layer of security controls that protect data at rest and in transit.
- Symantec Data Loss Prevention monitors email downloaded to mobile devices over Exchange ActiveSync and monitors and protects network communications sent from iPads and iPhones over Exchange ActiveSync, HTTP/HTTPS, and iOS apps like Facebook.



## USE CASE 5: OFFER SECURE ALTERNATIVES TO CONSUMER APPS

IT knows that many end users are already using consumer-grade apps to review and edit documents, take notes, and instant message/chat/text with co-workers. By allowing end users to use unapproved apps, corporate information is put at risk. IT is challenged to provide corporate approved solutions, while still trying to enable productivity.



### SAVO – A SYMANTEC SEALED PROGRAM PARTNER

“The impact to us is really during those IT conversations and security conversations where customers will ask us how we encrypt, or do you support remote wiping, do you deal with jail breaking and root detection across devices? It is very easy to say yes. Through our Symantec partnership, we can ensure that those are in place.”



#### IT CHALLENGE:

- How can I provide my users with a secure mobile workspace that lets them get their job done?
- How can I give my users a secure alternative to the consumer apps they use to store and share content/files?

#### SOLUTION:

Empowering your workforce with easy to use corporate-approved apps is the key to enhanced productivity without sacrificing security. Symantec Mobility Suite provides secure productivity apps including Symantec Secure Email and Symantec Secure Web. Secure Email, a Microsoft Exchange ActiveSync-based email app, allows secure syncing and storage of corporate email. Secure Web, a secure Web browser, provides safe access to internal Web-based applications and content. The Symantec Sealed marketplace, a rich ecosystem of secured third-party mobile apps, provides wrapped apps for document editing, file sync and share, note taking, and more.

#### HOW SYMANTEC MOBILITY SOLUTIONS CAN HELP:

- Symantec enables a secure mobile workspace by delivering a collection of secure and managed apps (e.g. Secure Email, Secure Web and third party Sealed apps) that seamlessly interact with each other.
- Symantec Mobility Suite provides integrated device and app management that allow companies to provide consistent security controls across popular mobile platforms such as iOS, Android, and Windows Phone.
- The Symantec Sealed Program empowers mobile app developers to join a trusted ecosystem of 3rd party, enterprise-ready apps that comply with app distribution rules.

## USE CASE 6:

### BLOCK MALICIOUS MOBILE THREATS

Employees increasingly rely on smartphones and tablets, both personally owned and company issued, to achieve higher levels of productivity. But, these productivity gains come with an expanded threat landscape, as mobile devices have become a target for cyber attacks. IT struggles to keep pace with the complex and fast-evolving mobile security scene. They are looking for mobile partners that understand how to maximize mobility's rewards while minimizing its security risks.



### A LARGE BEVERAGE COMPANY ADDS ANDROID

“By applying MDM and threat protection, we are able to manage the mix of device options favored by our employees. A solution which can make IT organizations worry less about what the underlying operating systems do or do not support makes even having Android more palatable”.



#### IT CHALLENGE:

- How do I protect my users, data and network from malicious mobile threats?
- How do I assess the risk behavior of an app and create policies for usage?

#### SOLUTION:

While MDM and MAM are critical components to a mobility strategy, extended security is essential to protect against mobile threats. This means it is necessary to implement mobile threat management to provide antivirus, anti-spyware, and anti-spam. By deploying comprehensive protection against threats such as malware, greyware, and risky apps, you can confidently embrace Android devices in the enterprise without compromising security. Leveraging cutting-edge technology from Norton Mobile Insight and the Security Technology and Response (STAR) experts, Symantec's threat protection delivers exceptional protection without slowing down device performance.

#### HOW SYMANTEC MOBILITY SOLUTIONS CAN HELP:

- Symantec Mobility: Threat Protection provides powerful, effective protection against malicious threats and unauthorized data access on Android devices.
- Leveraging our Norton Mobile Insight technology, Symantec provides smart and actionable information to employees about the potential privacy and performance risks an app poses.
- Through its Global Intelligence Network and Security Technology and Response (STAR) experts, Symantec sees, analyzes and masters the information within the threat landscape and provides unequaled threat protection, especially for users of open mobile operating systems (such as Android) that cannot enforce universal app screening.



## USE CASE 7:

### SUPPORT BYOD AND CYOD

With bring your own device (BYOD) and choose your own device (CYOD) programs becoming the norm, IT is struggling with how best to secure corporate data on personally-owned devices. Corporate-owned devices allow IT to standardize on a single OS, device image, and set of apps. But traditional device management introduces complexity by encroaching on user privacy and experience by enforcing control at the device level. BYOD and CYOD programs introduce multiple mobile platforms (e.g. iOS, Android, Windows Phone) with different management and protection capabilities. These programs extend beyond employees to enable partners and contractors.



### LACLEDE GAS COMPANY

“We wanted to be prepared and be on the front edge of bring your own device. We chose Symantec because of the way it would integrate with our existing infrastructure. It was no sooner than tablets were in the door and we had folks with a lot of critical data and they wanted to know what they could do with it on their tablets.”

#### IT CHALLENGE:

- How do I support the personally owned devices my users are using for business?
- How do I protect corporate data on personally owned devices without infringing on user privacy?
- I'm using mobile device management (MDM) to support BYOD and CYOD programs, but my users are leery of IT or the enterprise gaining control and visibility of their personal apps, data and device.

#### SOLUTION:

Symantec enables IT to apply a consistent level of security on personally owned, heterogeneous devices and platforms (e.g. iOS, Android, Windows Phone) from a single console. Symantec helps reduce the complexity of multiple mobile platforms with different management and protection capabilities by providing a flexible, comprehensive solution that does not compromise security or user experience. Secure data, deliver apps and content, and protect against threats with Symantec Mobility Suite.

#### HOW SYMANTEC MOBILITY SOLUTIONS CAN HELP:

- Symantec Mobility: Application Management (MAM) allows IT to enforce data protection policies on a per-app basis with our unique app wrapping technology. This provides clean separation of corporate and personal data on the device. IT can protect corporate data without infringing on user privacy or experience. Managing at the app level also allows IT to selectively wipe corporate data while leaving personal data untouched.
- Symantec Mobility Suite enables device choice by providing consistent security controls across popular mobile platforms such as iOS, Android, and Windows Phone.
- Symantec Mobility: Threat Protection allows IT to confidently embrace personally owned Android devices in the enterprise by providing leading-edge mobile security that protects against malware, greyware, privacy risks, fraudulent websites and other mobile threats.

