**Migrating from Good for Enterprise to VMware AirWatch: Building the Business Case**

BlackBerry’s announcement that Good for Enterprise will not be supported after mid-2017 means that customers of that legacy platform face a very difficult choice: Migrate to the new Good Work email app and the Good Dynamics platform, or select a more productive, lower TCO and identity-integrated solution designed for the long term.

With BlackBerry’s decision to eliminate Good for Enterprise from its product line, users of this platform face a challenge that must be addressed by August 17, 2017, the day the product reaches end of life. Whether users and IT managers are happy or not, a new solution must be selected. Organizations using Good for Enterprise must therefore undertake an analysis to evaluate current and future needs, decide on a new direction and begin the migration of both IT solutions and end-user bases.

An unnecessary burden? Probably. A huge effort? Perhaps. But there’s also a valuable opportunity here to change direction and move to new solutions that enhance productivity, improve reliability, offer more functionality and optimize the end-user experience—all with lower costs. Worth the time? Definitely.

A key and necessary element in this process, beyond the technical and operational evaluation of alternatives, is building the business case for the direction that will ultimately be selected and deployed. A business case defines the main justifications for selecting a winning candidate, and considers both essential requirements and financial impacts, along with their corresponding benefits.

Having a list of important criteria for building and defending this business case can ease the process. There are three key justifications that dominate the business-case framework: financial costs, organizational productivity and, most important, security. Assuming an organization can realize benefits in each of these three critical dimensions, the process of building a business case will be both enlightening and beneficial.
Enterprise mobility management: Understanding the costs

As noted above, certain fundamental costs involved in the forced migration process from Good for Enterprise simply cannot be avoided—the in-place solution is absolutely going away. A core objective for any replacement is to lower the total cost of ownership (TCO), as is always the case for any functional element in IT. Enterprise mobility management (EMM) is now mission-critical in most IT shops. While IT budgets are always tight, overall organizational success is essentially and fundamentally dependent upon a productive, secure and cost-effective mobile workforce. As a result, it’s essential that organizations understand and control the costs involved.

The TCO of any IT solution consists of two key elements: capital expense (Capex) and operational expense (Opex). Capex includes hardware, installation, upgrades and modifications; other one-time engineering, planning and logistics activities; and any other components or activities required to get up and running. Opex comprises everything else, including ongoing management, troubleshooting and remediation; user support and help desk; and updates and related work. Capex tends to decrease over time, as advances in technologies add value and competition holds down prices. Opex, on the other hand, is labor-intensive, so costs tend to rise unless steps are taken to improve productivity—an element so important to the business case that it’s one of our Top Three items and discussed in detail below.

On the Capex front, the rip-and-replace necessary here requires a detailed examination of the capital expense of required new infrastructure. Good’s suggested replacement, Good Work and Good Dynamics, can have increased server costs and thus significant costs related to acquisition, configuration and ongoing management. On the Opex side, key features and capabilities needed by specific organizations may be missing from Good Work and Good Dynamics (they’re fairly new and immature, after all), resulting in increased operational expense, especially with respect to end-user support.

Any organization dealing with the replacement challenge is well served by the consideration of alternative solutions. Rip-and-replace can indeed be daunting, but the benefits of a more functional, capable, robust and reliable solution can also more than justify the effort required—if the right alternative is selected, of course.

Optimizing user and IT staff productivity

Productivity can be a very complex concept, but with respect to the business case challenge we examine here, it means getting the most out of investments made in a new solution. This is particularly true for the productivity of the people involved, both in IT and the end users they serve. After all, IT fundamentally exists to enhance the productivity of staff across the organization, and any IT capability must be evaluated with regard to this goal. Optimizing productivity isn’t just about the financial benefits, by the way; productive solutions go a long way toward enhancing worker satisfaction, which always reflects positively on the customer experience overall. In short, the right IT solutions can make all the difference between successful organizations and those that struggle.

With respect to IT staff, productivity is maximized when solutions are easy to understand, administer, manage and support; ease of use is just as important to IT professionals as it is to end users. Complexity in every dimension must be minimized; for example, some solutions require multiple servers, multiplying the IT workload required to establish and maintain services. Troubleshooting is more complex. And, of course, Capex increases as more infrastructure is required. Solutions must also be open. For example, the use of proprietary application software containers may be preferred by some, but is no longer the only available option as mobile operating systems provide increased security capabilities (iOS Managed Apps and Android for Work, for example). Valid, viable and supportable solutions must steer clear of such increasingly antiquated impediments to productivity.

Similarly, end users need solutions that are easy to use, self-service and reliable. Given that a rapidly increasing
A number of organizations have become mobile-centric in an effort to improve staff productivity and customer responsiveness and service, solutions that are unreliable, immature or difficult to use simply get in the way, with adverse impacts across the organization as a whole.

**The most important issue of all: Security**

Finally, security is the third key element in building the business case required by the forced migration. Maintaining an appropriate level of security is beyond critical in every organization today. News outlets regularly feature stories about breaches and compromises to critical data—situations that are clearly never acceptable for organizations. The forced migration is thus a real opportunity to examine inadequacies in current mobile security solutions, and to de-risk mobile operations overall. Successful mobility management solutions, therefore, must have essential, comprehensive and reliable security capabilities built into the product from day one.

The following are some key security features that aid in a business-case justification:

- **Identity Management:** Identity management enables users to access a wide variety of applications and approved devices quickly and easily. It’s thus easy to control access to applications and data, ideally across local and cloud-based services, without compromising either security or end-user productivity. It’s also easy to authorize access to an enterprise app store using this capability.

- **Mobile Application Management (MAM):** Controlling access to sensitive data and limiting local apps to only those explicitly authorized are essential capabilities in contemporary security solutions, and MAM deals with the latter. Lifecycle control of apps is vital, from sourcing or developing to setting security policies, deployment, usage analytics and more.

- **Single sign-on:** SSO enables users to log in once and access any application service no matter whether the app is mobile, cloud, web or virtual; or if it’s local, behind the firewall or cloud based.

- **Access Flexibility:** Many users in the field and on the go require access behind corporate firewalls, and this has historically been cumbersome if not downright tricky. Advanced security solutions provide authorized users with automatic tunneling, while also assuring that only authorized apps have access.

- **Integration and Completeness:** Specific security requirements will of course be a function of local security policies. But solutions with the flexibility and robustness to provision all of the above, plus additional features such as network access control, anti-malware, e-discovery, archiving and more. It’s vital to consider security as an integral architectural feature, not an add-on afterthought.

**Conclusion**

There’s neither escape nor justification for delay: *Good for Enterprise is coming to end of life, and it’s coming soon enough that a strategy for replacement must be put in place quickly.* Now is a great time to look at current and future needs, TCO, operations and, of course, security in order to really understand EMM solution requirements, and to build these into the business case that ultimately drives the selection of a replacement. VMware AirWatch embodies the best combination of features and capabilities that optimize for lower costs, higher staff and end-user productivity, and the best security available, all adding up to long-term value.

The completeness of the AirWatch solution has been recognized by numerous analyst firms, and it makes good business sense to consider AirWatch as part of your organization’s due diligence in planning for EMM after Good for Enterprise.

For more information on why AirWatch offers a more cost-effective, productive and secure option, please visit www.air-watch.com/lp/goodsafepassage.