IBM Security
Thought Leadership White Paper

When business is the app, the app is the business

Volume II: Four components of a solid mobile app strategy

IBM

Introduction

IBM Security, a leader in Enterprise Mobile Management (EMM), presents Volume II of a three-part series that explores the appification of the enterprise, including IT's role as the great enabler.

In this volume, learn how to design a business-driven app strategy that advances business goals – without putting enterprise data and your network at risk.

Business appification consists of discovery, scalability, sustainability and security.

Four components of a solid mobile app strategy

As we discussed in *Volume I, The Appification of Business*[1], mobile applications are fundamentally changing the way businesses engage with employees and customers and the general manner in which business is done. Building an effective strategy is key to making sure that apps truly benefit the business while protecting your corporate data and network.
A successful approach to appification should involve discovery, scalability, sustainability, and, of course, security.

Build the apps that your users need

According to a survey of 300 senior enterprise mobility pros that was created by the Enterprise Mobility Exchange (EME)[2], enterprises are primarily focusing their mobility investments on mobile apps to improve employee productivity.

It sounds like the same old story, different platform. Management wants employees to be more productive, improve customer engagement, and make their work and lives easier. IT wants to make sure that employees does not wreak havoc on the network and expose the company to major security risks (and costs). However, building a mobile app-based business is not supposed to be a Business versus IT showdown. In fact, it is critical that IT and Business work together to develop the strategy.

First, IT needs to know the overall business objectives of any app-enabled initiative. Then, they need to spend time with both management and users to understand how people – customers and employees – use their devices to interact with each other and access the information they need, what information they consume and share, and what issues might be getting in the way. This process should occur across business units and use cases – even for the development of a single app – to avoid gaps and inconsistencies in the finished product. Working together with the business side, IT needs to analyze:

- What will they be doing with it? Will it be used for direct customer engagement?
- What features are most important?
- What functionality will make that possible?
- What systems will be accessed?
- What security risks will the app pose? What could happen if it was accessed by an unauthorized user?
- Are there data regulations to consider?
- What value do we expect this app will bring?

Ready to scale at a minute's notice

Once the initial analysis is complete, IT can flesh out a plan for developing and deploying the app. Regardless of the size or usage initially outlined, it is important to create a mobile app that is ready to scale to larger volumes while delivering an excellent experience. When choosing the technologies behind your apps, use the following considerations to think about the end result infrastructure:

- How can I make sure that my app offers a consistent user experience across devices and operating systems?
- Can my application architecture accommodate a variable number of users on demand?
- What will happen to our network when the back-end interfaces are linked to additional systems and/or databases concurrently?
- Is our network robust enough to allow for an increasing number of simultaneously connected devices?
- How will I monitor for bottlenecks during design, deployment and usage?

Change is inevitable

Over time, apps need to be updated, so you need to think long term. Unlike web apps, which reside on a server, mobile apps live on devices. That means that regular, quick changes to an app are not a possibility. Whether driven by fluctuating user demands or operating system (OS) updates, changes will be necessary, and achieving app sustainability requires IT to consider:

- Is the front-end app functionality adaptable enough to include new features requested by users?
- Will we be ready with zero-day updates to accommodate users immediately upgrading their OS?
- What is our process for user app collaboration and discovery?
- Are we ready to address user feedback for continuous design and development?

Security in every step . . . not as an afterthought!

In our next volume, *Addressing the Dangers of Appification*, we will discuss the last – but certainly not least – consideration in supporting the appification of business security.[3] Mobile apps are increasingly sources of corporate security vulnerabilities, due to poor data storage practices, malware, unauthorized access, lack of encryption and data leaks.

Gartner forecasts that 75 percent of mobile applications will fail basic security tests through 2015 and could offer an entry point for hackers looking to breach an enterprise's network.[4] The recent Masque Attack[5] overwrites an official enterprise app with a malicious app that is seemingly undetectable on a user's device because it masquerades as the original app.

As the appification of business spreads, so too will the threats to corporate data and the network. Thinking about – and applying – security measures needs to occur in every step of development and deployment.

In conjunction with the other solutions of the IBM® MaaS360® portfolio, MaaS360 can empower you to create a mobile application strategy that advances the business while providing scalability, sustainability and security. Contact IBM today to learn more about making the most of your enterprise's mobile app world.

Are you ready for the appification of your business? Check out the rest of this series:

- **Volume I:** ***The appification of business.*** Explore the appification of the enterprise and IT's role as the great enabler of app-led employee productivity and collaboration, enterprise growth and customer engagement.
- **Volume III:** ***Addressing the security dangers of appification.*** Understand the technical and practical considerations for successfully enabling and protecting the enterprise while building and implementing an app-based business.

Related resources

- Mobilize Your Corporate Content and Apps[6]
- Good Apps, Bad Apps: The ROI of Creating Exceptional Mobile Moments[7]
- Four Tips for Protecting the Enterprise Against Mobile App Threats
- Best Practices for Mobile Application Lifecycle Management[8]
- Webinar: Design, Develop and Deploy Mobile Apps
- IBM® MaaS360® Mobile Application Management

About IBM MaaS360

IBM MaaS360 is the enterprise mobility management platform to enable productivity and data protection for the way people work. Thousands of organizations trust MaaS360 as the foundation for their mobility initiatives. MaaS360 delivers comprehensive management with strong security controls across users, devices, apps and content to support any mobile deployment. For more information on IBM MaaS360, and to start a no cost 30-day trial, visit www.ibm.com/maas360

About IBM Security

IBM's security platform provides the security intelligence to help organizations holistically protect their people, data, applications and infrastructure. IBM offers solutions for identity and access management, security information and event management, database security, application development, risk management, endpoint management, next-generation intrusion protection and more. IBM operates one of the world's broadest security research and development, and delivery organizations. For more information, please visit www.ibm.com/security

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
March 2016

Please Recycle

1 IBM Security, *When App Is The Business, The Business Is the App Volume I: The appification of Business*, 2015, http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=WGW03105USEN&attachment=WGW03105USEN.PDF

2 Westacott, Robbie, *The Global State of Enterprise Mobility Report 2014/2015*, Enterprise Mobility Exchange, December 3, 2014, http://www.enterprisemobilityexchange.com/the-global-state-of-enterprise-mobility-report

3 IBM Security, *When App Is The Business, The Business Is the App Volume III: Addressing the Security Dangers of Appification*, 2015, http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=WGW03107USEN&attachment=WGW03107USEN.PDF

4 "Gartner Says More than 75 Percent of Mobile Applications will Fail Basic Security Tests Through 2015", Gartner, September 14, 2014, http://www.gartner.com/newsroom/id/2846017

5 IBM Security Intelligence, Four Tips for Protecting the Enterprise Against Mobile App Threats, February 11, 2015, https://securityintelligence.com/four-tips-for-protecting-the-enterprise-against-mobile-app-threats/

6 IBM Security, *Mobilize Your Corporate Content and Apps*, 2015, http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=WGW03111USEN&attachment=WGW03111USEN.PDF

7 "Good Apps, Bad Apps: The ROI of creating exceptional mobile moments," an IBM-commissioned paper by Forrester, IBM MobileFirst, 2014, http://www.ibm.com/mobilefirst/us/en/good-apps-bad-apps.html

8 IBM Security, *Best Practices for Mobile Application Lifecycle Management*, 2015, http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=WGW03110USEN&attachment=WGW03110USEN.PDF

WGW03106-USEN-01