Infrastructure Solutions International

Enterprise Mobility:
Securing a mobile oriented enterprise

Introduction

Mobility and wireless communications are critical areas to an enterprise moving forward. As enterprises become cloud, connected, and data oriented, they need to be conscience of the rapidly changing threat landscape. Change is not limited to technology, but it also includes business processes around business continuity/disaster recovery (BCP/DR), risk assessments, network security, and data security.

We are seeing changes across a number of technology areas all at the same time. This puts organizations in the situation of constantly shifting priorities.

Our intent is to guide organizations through the changes to a secure mobile enterprise by outlining a framework for evaluating solutions.

Market Drivers

An extended enterprise is the shift in the access of corporate resources from anywhere and, potentially, at any time. Mobility isn't new to the enterprise; it's just the mobile and wireless technologies have transformed the business.

The revolution in enterprise mobility happened fast. It forced business leaders to react swiftly to accommodate change. Three market drivers assisted in the rapid reaction.

Cloud computing

The change in computing infrastructure has allowed enterprises to adopt new technology at a quicker pace. Now, an organization can take advantage of public, private, or hybrid clouds in numerous ways to align IT with strategic goals.

Consumerization of enterprise mobility

With Apple iOS and Google android growing at rapid rates in the consumer market, it was only a matter of time before employees began to require that same user experience at work. With the explosion of mobile applications and endpoints connecting to an enterprise, employees have essentially forced organizations to evaluate their IT infrastructure to accommodate mobility. The irony is that, as cyber security threats continue to evolve, more emphasis on risk management strategies are important.

Big Data

With the growth in data being processed and analyzed, we are at a point where decisions are more data-driven than ever. Being able to manage the volume, search, and analyze are key to businesses maintaining competitive advantages.

Challenges

The change in enterprise mobility has led a lot of organizations going down the path of looking for quick fixes. Applying a quick fix to a complex problem leads to issues later. The previous approach to mobility management no longer works in a world of bring your own device (BYOD), corporately owned, personally enabled (COPE) and choose your own device (CYOD). We are now in a device and platform agnostic environment that requires security end to end. Businesses need to think about more than just the device, which has exposed other areas within their IT environment.

1) **Enterprise mobility Management (EMM)**

   Initially, the thought was enterprise mobility is primarily about device management. If we can control the device, we are secure. That's where businesses quickly turned to enterprise mobility management (EMM) providers to solve the problem for device control functions and over-the-air (OTA) configurations. Mobile management now has grown to more than securing the device. While EMM started as device management, it now includes mobile application management, email management, and information management. To get complete security that is needed for mobility, most EMMs leverage a partner ecosystem. This leaves businesses evaluating a broad set of technology options where requirements are a moving target.

2) **IT Infrastructure**
   Think about your internal and external operating environment. The infrastructure needs of the business are unique, and there are plenty of options.

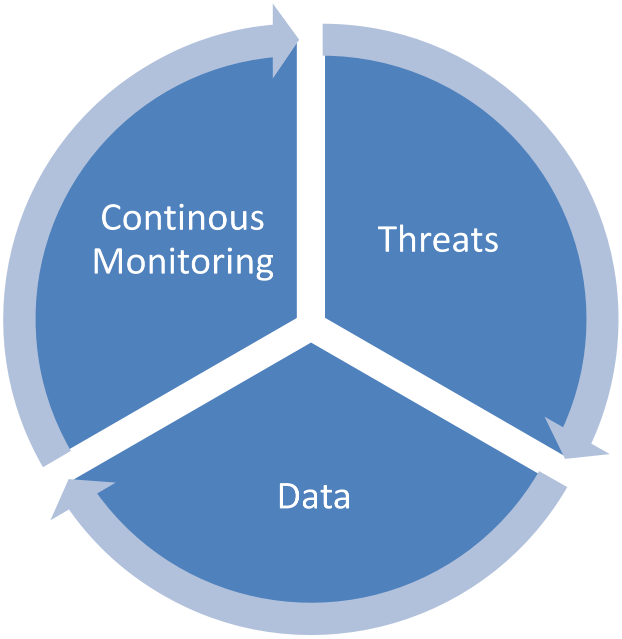
   From a computing standpoint, the number of servers and applications being used by a business is growing. The cloud has made asset management a unique task due to the potential location of corporate resources being in several operating environments.

   From a network standpoint, mobility can leverage either wired or wireless network access. However, the majority of the new endpoints (i.e. smartphones and tablets) that are attaching to the network, leveraging wireless technology. However, the network consists of more than wireless components; it also includes firewalls, switches, controllers, routers, intrusion detection/prevention systems (IDS/IPS), and so on. Securing the network is typically a large task in itself, but now it includes a variety of operating systems that need access.

Applications are a mixture of web and mobile. The issue is backend requirements for the applications are different. Depending on your business applications (internal, pubic, or purchased) your software development and deployment strategy might experience changes.

3) Risk management

Enterprise mobility risk management can be categorized into three areas: understanding threat attack vector, assess based data, and continuous monitoring. To secure your enterprise allocating resources to security management is essential. There isn't a simple answer to this, as each organization and industry is different.



- Threats – a complex environment that includes advance persistent threat (APT) attacks, zero day attacks, various mobile platforms, etc.
- Data – data breaches are happening frequently. Data management strategies include understanding data at rest, data in transit, DLP, etc.
- Continuous monitoring – threats changes, strategies change and processes need to be re-evaluated

4) **Lifecycle Management**

Enterprise infrastructure, devices, applications, and security risks all have different lifecycles. The approach to managing and supporting each one is different. Dealing with the lifecycle individually, will lead to problems that can harm your business.

Securing the mobile enterprise

Knowing the potential challenges, an integrated end to end solution is needed. This is defined as a bi-directional experience from users all the way to the data source. To begin securing your enterprise think about what your mobile IT operating environment looks like. Documenting this operation allows a business to understand users, devices, applications, and data within their organization.

Now, we have the data to start identifying technical solutions solve your problems. Frame your requirements around these 10 areas.

1. Security – The threat landscape for mobility consists of insider and external threats. A solution needs to map the security policy that has been developed based on a risk assessment. Ensure the solutions provide monitoring and management capabilities to handle both inside and outside threats.
2. Data – Not all data is the same. Classify your data to ensure that a solution provides the data security you need to secure your enterprise.
3. Network/Wireless – assume data, video, and voice applications will be used. In general, a lot of smartphone or tablet traffic will be over the cellular network, but if it's over your WLAN, ensure your network is mobile ready.
4. Scalability – the ideal situation is that, as you grow, there are no issues related to the operating environment. Ensure that a solution can grow as your organizational needs develop.
5. Partnerships – right now, the majority of solution providers for mobility and wireless have technology partnerships. Knowing this saves time in building a secure integrated solution.
6. Architecture/Design – security is different for cloud vs on premise solutions. Understand your options to ensure you are comfortable with the various risks.
7. Mobile device platforms – three platforms currently dominate the market: android, iOS, and windows. Determine what your needs are and then correlate that with the applications, enterprise security requirements, and EMM device support.
8. Support – This is something that is usually discussed after the implementation, understand the support processes, model, etc. Then select one that suits your needs.

9. Users – not all users are the same in respect to data access. Ensure access controls and identity management capabilities are available. Two-factor authentication would be ideal but evaluate it carefully so it doesn't impact user's productivity.
10. Management –Ensure your staff has the skills to manage the systems and stays abreast of the latest security threats.

Solution

Breaking down your mobile IT environment now puts you a unique place to adapt to enterprise mobility and wireless. Solving the problem end to end allows you to classify the operating environment around three activities: Assessment, Implementation, and Management. You can jump around to each area, but a holistic approach is being used to secure your business.

The value in this approach is that, as a business, you have control of this moving target, but it also enables you to benefit from a controlled vendor selection process, risk management process for a large threat environment, data intelligence, scalable processes, and governance/compliance strategy.

Conclusion

As we mentioned at the beginning, adapting is important in this new era of enterprise mobility. Now, it's time to reflect on where you are as an organization. There will be a mobile component that is associated with your business. There will be new systems, migration of legacy systems, and more. However, organizations need to get proactive in securing it, to prepare for the next phase of enterprise transformation. The internet of things (IOT)/industrial internet of things (IIoT) efficiencies that will be realized will also include mobility. Securing the mobile-oriented enterprise now with this framework allows you to explore future opportunities in a structured manner.

About us

Infrastructure Solutions International is a mobility and wireless solutions provider. With technical staff experienced in cloud, networking, mobility, security, and wireless we have the expertise to solve your problems.

Infrastructure Solutions International
www.infra-si.com
info@infra-si.com