Honeywell | Enterprise Mobility

BEYOND MDM: A MULTIDIMENSIONAL MOBILITY STRATEGY

Why device-centric strategies no longer meet today's mobility needs

Abstract

The number of mobile workers is growing exponentially, expanding the potential for productivity while introducing new challenges for corporate IT leaders. As the volume and variety of devices in the enterprise expand, these challenges have only become more complex. Device-centric management strategies have prevailed over the last several years, but this approach can no longer keep pace with the increasing number of remote workers who need to access more applications across multiple platforms. Enterprise IT leaders must shift from locking down devices to securing the corporate applications, data and other proprietary content that reside on these devices. In short, they need to move beyond mobile device management to a more holistic management method.

Table of contents

Introduction

When thinking about enterprise mobility management, it is worthwhile to consider how rapidly the use of mobile devices has evolved. In the span of a few short years, the device market has become increasingly competitive and sophisticated. The enormous uptake of powerful smartphones and tablets for personal use – coupled with a pervasive shift toward more flexible work styles – has made the bring-your-own-device (BYOD) trend a reality; and this trend, in turn, has prompted a surge in demand for mobile access to corporate systems and data.

All of these factors have placed mounting pressure on corporate IT departments to find new ways to balance flexibility and user satisfaction with standardized security practices. The prevailing response has been to focus on monitoring and controlling the devices themselves. This has led to the emergence of a host of mobile device management solutions, which continue to provide a strong foundation for securing mobile environments and tracking mobility performance over time. But persistent use of personal devices to access corporate networks and growing demand for mobilizing business processes have significantly altered the mobility landscape. As a result, business and IT leaders need to make finding a more holistic approach to mobility management a top priority.

The Promise of Mobile Productivity

These three factors – growing preference for mobility, more versatile and powerful devices and access to high-performance wireless connectivity – are coalescing to create the potential for greater productivity.

The case for investing in enterprise mobility is often tied to anticipated gains in employee productivity. The logic follows that, by making it more convenient for employees to remotely connect to corporate resources, regardless of location, they will be able to get more done. In fact, a recently published report highlights a tendency among employees who rely heavily on mobile devices for work to willingly work longer hours during the week.[1]

The mass adoption of smartphones and tablets in recent years has had dramatic and lasting consequences for enterprise IT organizations. Now, more than ever, employees across practically every line of business access and share information while on the go. According to one estimate, 40 percent of the world's total workforce will be mobile by 2016.[2] And industry analysts expect that number to grow. In addition, numerous surveys show that respondents have expressed their eagerness to embrace mobility to achieve greater work/life flexibility. And advances in device technology and wireless connectivity provide the infrastructure needed to support this work-from-anywhere model.

These three factors – growing preference for mobility, more versatile and powerful devices and access to high-performance wireless connectivity – are coalescing to create the potential for greater productivity. Companies of all sizes are looking to harness these trends to boost their competitive edge by empowering employees to share information more easily across multiple locations.

Alongside these major catalysts for increased mobile productivity are several related developments that have been steadily gaining momentum. First, today's workers are generally more comfortable connecting virtually with colleagues. Similarly, they have become increasingly accustomed to accessing business applications that are based on a software-as-a-service (SaaS) model. Many view mobility as a way to extend the flexible workstyle benefit that this software model provides. Finally, modern workers are generally more adept at shifting among multiple devices, including laptops, smartphones and tablets, depending on the task at hand. Most are happy to use their own devices for work.

These trends reveal distinct opportunities and challenges for IT leaders. For example, the ability to access critical applications at a moment's notice – anytime, anywhere – can certainly result in increased productivity. At the same time, the prospect of employees using multiple personal devices to connect to sensitive corporate data represents a formidable IT management challenge.

1. iPass, 2012
2. Gartner, 2012

The Increasing Complexity of Mobility Management

The well-established connection between mobility and productivity goes to the heart of why managing mobile environments can be so daunting. For employees, mobility supports the worthy drive to find information faster and eliminate hurdles to decision-making. Yet IT must balance user expectations with the need for standardized security controls to protect against data breaches and meet regulatory mandates. The trick is to stay out of the way of productivity and innovation, but still lead when it comes to network-access control and data security.

The bring-your-own-device (BYOD) trend has become a movement – and a business reality. All things considered, BYOD offers a lot of promise, but it does present some obvious challenges when you're trying to balance flexibility and security. We'll examine the specific role that BYOD plays in mobility management. But in rolling out any enterprise mobility solution, there are a number of objective factors that IT leaders must confront irrespective of the BYOD dilemma. Some of these include:

Security and Identity

Ensuring rigorous identity and access management is not a unique challenge to mobility environments. And to date, mobile device management (MDM) solutions have filled an important need in helping enterprises manage remote endpoints. But not all MDM solutions have kept pace with the rapid evolution of mobile operating systems and the devices themselves, exposing vulnerabilities that can only be met by a more complete set of management capabilities.

Device Fragmentation

The device market continues to grow more diverse each year, with new releases and form factor variations emerging at a rapid pace. The ever-changing combination of carriers, features, operating systems, configuration options and connectivity services adds layers of complexity for IT managers and can lead to frustration among employees, who simply want to connect to the corporate network while on the move. The tendency among a growing number of employees to use multiple devices only compounds these challenges.

App Development

As modern enterprise mobility reaches critical mass, the demand for mobile business applications continues to soar. Keeping pace with this demand is a challenge all by itself, not to mention finding the resources to tailor apps to specific business processes and make them available across multiple device types and operating systems. Usability is also an issue, as desktop web applications do not necessarily function well on tablets.

Infrastructure Investments

In a world where users expect nothing less than pervasive, "always-on" connectivity, many IT leaders are finding that their wireless network infrastructure is not prepared to handle increased traffic. Beyond capacity constraints, administrators need to grapple with the reality that most wireless systems were not engineered for business-critical workloads. Configuring wireless networks for fault tolerance adds cost and management time. With the promise of SaaS, users expect to access all corporate data from anywhere they have an Internet connection. Legacy business systems may not be up to the task without additional investments.

The Impact of BYOD on Mobility Management

Although BYOD can add complexity to mobility management, a coherent BYOD policy can increase user satisfaction, enhance productivity and drive innovation. While that will help add value to enterprise mobility, it probably won't make it easier to manage. According to Gartner, the unexpected consequence of BYOD programs is a doubling or even tripling of the size of the mobile workforce.[3]

Personal devices can be at a higher risk of exposure to malicious software (malware) through rogue mobile apps. Even if this exposure is unaffiliated with business use of the device, it can be inadvertently introduced to corporate networks.

To support device choice, enterprises must be prepared to manage a greater variety of operating systems, mobility services, carriers, form factors and feature sets. The high degree of fragmentation in the mobility market is amplified by BYOD, which will influence security and management overhead. IT organizations will likely expend more resources evaluating personal applications for support on corporate networks and managing bandwidth consumption when remote employees use multiple personal devices simultaneously.

3. Gartner, 2013

Why Mobile Device Management Is Not Enough

MDM solutions are purpose-built to monitor endpoints. Many of these solutions do not sync with the role-based access functionality of enterprise identity management systems. This makes it more difficult to enforce security policies in a consistent way for mobile users who need to move among devices.

Over the past several years, MDM solutions have emerged as the main way of mitigating these risks. The intent of MDM is to manage and secure the endpoint itself, providing encryption for data at rest on the device. Typically, organizations have used MDM solutions in combination with device-level virtual private network (VPN) functionality to provide security for data in transit between the device and the corporate network.

However, there are several shortcomings with an approach that focuses primarily on securing the device. First, MDM does not adequately address the realities of BYOD environments. Employees who use personal phones or tablets for work chafe against the idea that IT can impose full control over their devices at all times. Because MDM solutions target the device, and not the applications and data on the device, employees fear losing personal information. One common scenario involves employees who leave an organization only to find out that they have lost family photos or other personal content when their former employer remotely wiped their device to remove enterprise applications.

Another limitation of an MDM-only strategy is that it does not efficiently deal with the use of multiple devices by a single employee. MDM solutions are purpose-built to monitor endpoints. Many of these solutions do not sync with the role-based access functionality of enterprise identity management systems. This makes it more difficult to enforce security policies in a consistent way for mobile users who need to move among devices. Ultimately, the real endpoints are people, and recent research shows that one in ten employees do not use any password or PIN to control access to their devices, and almost half access sensitive corporate data through their mobile devices on unsecured public networks.[4] It all adds up to IT administrators spending more time on security management tasks.

Finally, most MDM solutions by themselves do not sufficiently protect corporate data that is accessed and stored in the cloud. For example, in the absence of a robust enterprise content management solution, employees frequently turn to cloud-based media sharing and collaboration services to send large files. In fact, many of the latest devices integrate these services into the operating system, making them readily available to use, and sometimes even hard to avoid. Of course, administrators can set up their MDM solutions to blacklist these services. But this only adds to the list of items they need to track each day and can stymie workers who are simply trying to find ways to stay productive.

4. Osterman Research, 2014

A Holistic Approach to Mobility Management

It is clear that enterprise mobility is growing and becoming more complex; more than half of CIOs report strong employee demand for a wide range of mobile devices, and almost a third predict that laptops will soon be replaced by tablets.[5] The time has come for enterprises to take a multidimensional approach to mobility management – one that combines device security, application management and content protection in a single, unified vision.

Mobile application management (MAM), which covers many of the gaps left by MDM solutions, should be an integral component of any mobility management strategy. By focusing on controlling access to specific applications, MAM adds a layer of protection. Also, by enabling a cleaner separation between personal-use apps and corporate apps, MAM addresses BYOD in a more reasonable, real-world way, which can lead to higher user satisfaction and productivity. Finally, MAM solutions help to simplify management and security by automatically distributing and updating corporate apps based on user roles within an organization. As a result, employees can always count on access to the latest, fully secured versions of apps across all of their devices.

As businesses seek to provide remote employees with a full-fidelity, highly secure work experience on mobile devices, they are recognizing the important connection between mobile content management capabilities and employee productivity. Mobile content management (MCM) solutions can prevent the exposure or loss of sensitive information by moving content from corporate file shares to a secure centralized "container." Only users who have proper credentials can access that content through their mobile devices.

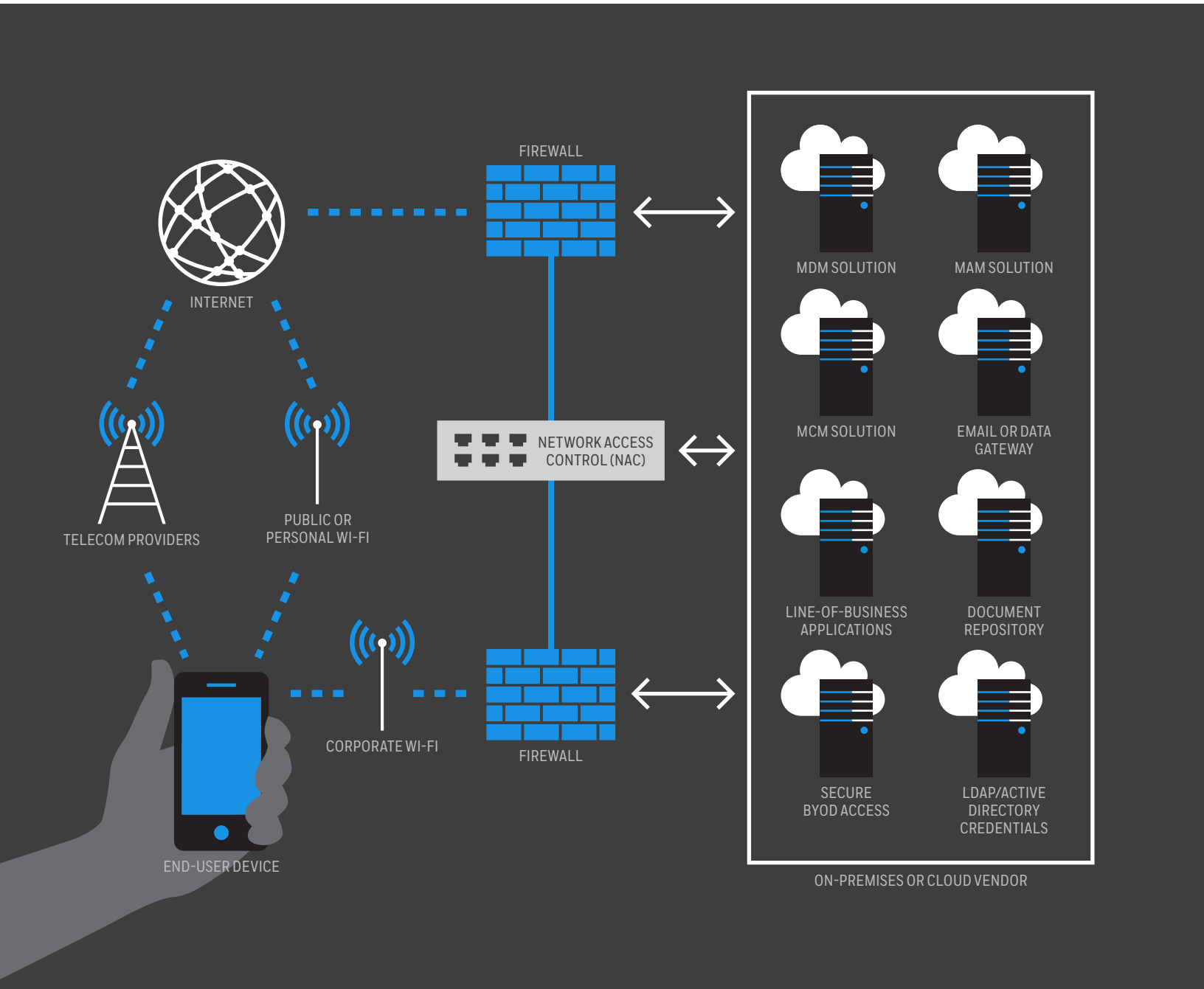
New services have also arrived that provide mobile application risk assessments. This combined with a MAM/MDM solution can be quite powerful and provides more insight into consumer applications that could pose security threats. The IT administrator can set his own threshold and automate the compliancy functionality. For custom applications, several MAM solutions now also provide APIs, so custom in-house applications can benefit from features such as secure access to internal resources, single sign-on, additional authentication, data loss prevention (DLP) and secure data containerization.

With so many mobile devices being brought to work, there is also an increased need to protect your internal networks from rogue devices and devices that are not fully managed. Network access control (NAC) solutions can assist in protecting and creating a perimeter around your most critical virtual local area networks (VLANs). Perhaps corporate-managed devices should have different access than BYOD devices, for example. NAC solutions can also tie directly to your MDM solution.

5. McKinsey, 2012

Moving Beyond MDM

Together with MDM solutions, advanced mobile security strategies incorporate solutions for application management, content management, secure internal access and identity and access controls.



The Benefits of a Multidimensional Strategy

While MDM solutions provide a cost-effective way to configure and manage devices at the highest level, complementary solutions can ensure that the applications, data and content accessed by and stored on those devices remain secure.

Recent research indicates that 72 percent of IT executives say they plan to spend more than 20 percent of this year's budget on mobility.[6] By implementing solutions that address security at every level of engagement between mobile devices and corporate networks, enterprises can achieve a number of important benefits to help make the most of their mobility initiatives:

Maximize Data Protection

By employing MDM, MAM and MCM solutions as part of a comprehensive, long-term strategy, businesses can maximize data protection. NAC solutions can even provide security on the network level. While MDM solutions provide a cost-effective way to configure and manage devices at the highest level, complementary solutions can ensure that the applications, data and content accessed by and stored on those devices remain secure.

Standardize Endpoint Management

An approach to security that targets mobility infrastructure in a holistic way also enables companies to standardize endpoint management across device types and platforms. This conforms to trends like fragmentation in the mobility market, BYOD and the increasingly common use of multiple devices to get work done.

Improve Mobile Productivity

Businesses that invest in optimizing for mobility can enable employees to safely use their personal devices for work and remove barriers to remotely accessing and sharing documents on the go. As a result, these companies can empower employees to boost productivity from anywhere.

6. Honeywell, 2014

Conclusion

It is clear that modern mobility management needs to adapt to the rapid pace of change in the mobility market. This evolution must include adoption of a more holistic approach to balancing security and productivity mandates. While MDM solutions provide a solid foundation for managing the configuration, deployment and monitoring of wireless devices, enterprises need to address security at every level – from the device to the applications, data and content that reside on these devices. As more employees rely on wireless devices in the workplace, a multidimensional management strategy will be the key to unlocking the promise of greater mobile productivity.

Need help with your mobile security strategy?

As a leading managed mobility services (MMS) provider, Honeywell can help you create a security strategy from the ground up, or optimize your existing plan. Find out how we can help.

For more information
www.honeywell.com/enterprisemobility

Honeywell Sensing and Productivity Solutions
9680 Old Bailes Road
Fort Mill, SC 29707
800.582.4263
www.honeywell.com

Beyond MDM WP | Rev B | 01/16

Honeywell