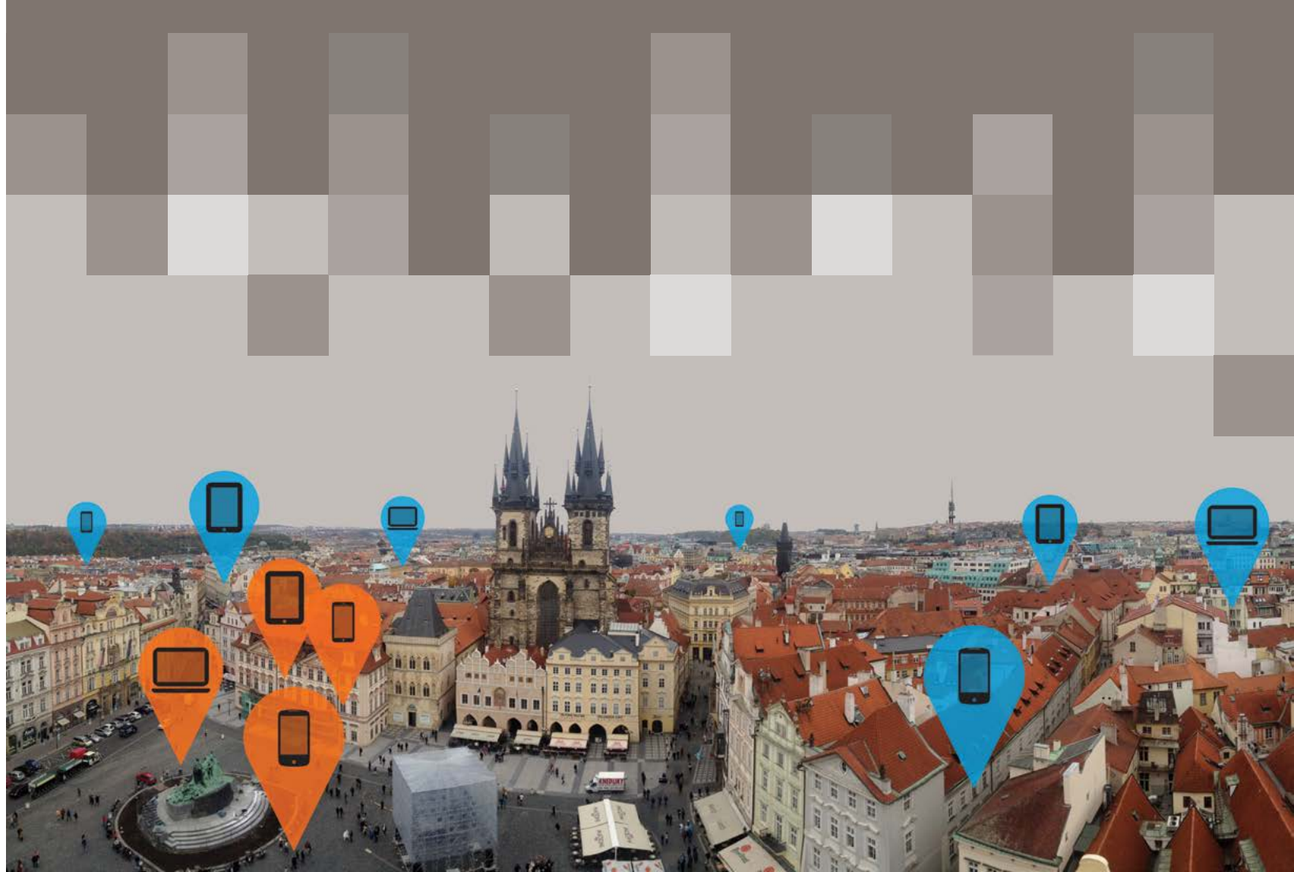
SKYHOOK®

Increasing Value of Your Mobile Device Management Solution

TABLE OF CONTENTS

INTRODUCTION

Mobile device management (MDM) will mature in 2014, growing into a $1.6 billion industry according to Gartner Inc.* and over the next five years, 65 percent of corporations will adopt MDM to address security concerns from smartphones and tablets.** MDM is growing as bring-your-own-device (BYOD) becomes a workplace norm and mobile security is now a necessity for businesses of all industries and sizes. According to a Cisco report,*** 70 percent of IT professionals believe the use of unauthorized programs results in as many as half of their companies' data loss incidents. Thirty-nine percent of IT professionals said they have dealt with an employee accessing unauthorized parts of their company's network.



The MDM industry is quickly becoming the new standard for IT. Providers with holistic solutions--that fit not only into existing technology platforms, but into their end users' lives--will thrive in 2014. Location technology will play a significant role in MDM in the coming years as it evolves beyond basic device tracking to create new features and opportunities for integration with other business technology. In the coming years of mass integration with IT, location will help MDM providers tackle a number of enterprise challenges.

Device-level location can add advanced functionality and valuable insight for MDM providers looking to scale operations and expand their feature sets for new markets. For example, MDM providers can integrate themselves with third party apps by exposing location data through an API. They can offer better data security by certifying that devices are located inside of designated safe areas. Geofencing empowers IT administrators to set secure geographic boundaries, triggering security procedures when a device enters or leaves the area.

The Rise of Mobile Devices in the Workplace

64% of companies have adopted BYOD

53% of employees use their own device for work

49% of companies are unaware of how employees access company data

Source: Rapid7 report

These added features are differentiators for MDM providers, and enable new revenue streams. Like the MDM market itself, location technology will establish new standards for device security.

SKYHOOK®

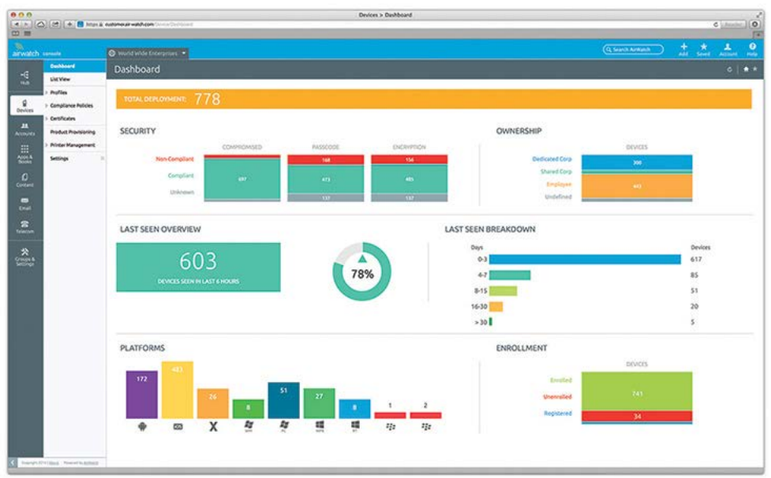
Chapter 1

Why Precise Location Makes a Difference

CHAPTER 1
WHY PRECISE LOCATION MAKES A DIFFERENCE

Often, MDM providers rely on broad city-level location data sourced from IP addresses, but precise location makes a difference. Knowing whether users are in the office or at home is a core function of today's BYOD programs. If users live close to where they work, an MDM platform without precise location can not deliver the necessary security based on the user's environment. Accurate location enables a better user experience for MDM clients and end users.

BYOD brings mobile phones, tablets, laptops and even wearable devices into the workplace. Blake Brannon, Senior Sales Engineer at AirWatch says, "Machine-to-machine and the Internet of Things (IoT) are both advancing very quickly. We're seeing peripheral devices, like smart watches, [smart] glasses and cars come to life in the mobile ecosystem. As more and more of these devices adopt smart technology and connect to one another, we'll see an increasing need for security – both at an enterprise and user level."



AirWatch browser view

As new devices and platforms emerge, MDM providers must adopt the out-with-the-Blackberry-and-in-with-the-new policy. Many MDM providers use the native location offered on the device; However, many of these devices may not have GPS. When employees need remote access to work resources, their precise location makes a significant difference.

How Hybrid Location Improves Current MDM Standards

IP network topology is the most common method of accessing a device's location (when GPS and Wi-Fi are not available). Yet IP location through network topology yields severely less accurate location data than GPS and Wi-Fi positioning.

"Machine-to-machine and the Internet of Things (IoT) are both advancing very quickly. We're seeing peripheral devices, like smart watches, [smart] glasses and cars come to life in the mobile ecosystem. As more and more of these devices adopt smart technology and connect to one another, we'll see an increasing need for security – both at an enterprise and user level."

Blake Brannon
Senior Sales Engineer
AirWatch

7:45am
Jen is working at a coffee shop with her MDM-enabled laptop and phone.

8:30am
She forgets her laptop when she leaves. The MDM software detects that her phone is no longer near her laptop, and that both are away from her office.

8:40am
The MDM software remotely locks the laptop, securing its sensitive data from Jen's employer.

9:30am
Jen realizes her laptop is missing and returns to the coffee shop to find it stolen.

9:40am
Jen alerts her company of the theft, but thanks to advanced location technology, the MDM solution already secured the sensitive data on it.

Network topology is a volatile method. IP location providers assign random latitude/longitude points within broad geographic areas, based on block-level IP information. This causes a large error radius and makes location data less accurate and actionable. Another problem arises from the mobile nature of IP addresses--they are not consistent with one location from day to day. An IP address could be shown in one location today, but appear in a different location tomorrow.

The superior alternative to network topology is hybrid location. Combining Wi-Fi positioning, GPS, cell tower, IP, and device sensor data intelligently yields the most precise location data. By using hybrid location, you can return the fastest time-to-fix location with the lowest power consumption.

By delivering precise location instantly, providers can verify that a device is in the realm of compliance within a second, and

offer a frictionless end user experience

for employees of MDM customers.

Additionally, this method is far more accurate and reliable than IP location. By delivering precise location instantly, providers can verify that a device is in the realm of compliance within a second, and offer a frictionless end user experience for employees of MDM customers.

AirWatch desktop view

Use Case: Precise Location Yields Better Security

A financial company that is concerned about their employees' devices being stolen could benefit significantly from an MDM provider that uses hybrid location. The financial company can set rules for remotely locking or wiping laptops that are taken outside of a secure area and are a given distance from the employee's mobile device for a given amount of time. This way, the company's data is secured before the employee even realizes their laptop is gone.

Hybrid Location Certifies Device Location

Another advantage to hybrid location is that it combines location sources. This method increases the confidence that the device location is not being spoofed or artificially manipulated. For example, devices that rely only on IP address for location can be vulnerable to IP proxies. And devices that rely only on GPS are susceptible to fake GPS coordinates. Web apps that rely on W3 browser location fall victim to users who manually fake their location through the DOM.

Hybrid location can guarantee a confidence score for accurate location by combining and comparing different location sources. The MDM providers can offer the ability to decide how confident their customers need to be with a location request before remotely locking or wiping a device.

Hybrid location even works when a device is not connected to the Internet.
If a device is not online it can still scan for nearest Wi-Fi networks, determining if the device is where it is supposed to be. If a device is out of a secure area, MDM providers can remotely lock or wipe the device of sensitive information. Additionally, once an employee's device is reported as stolen, the device can cache its location path, and communicate where it's been once reconnected.

How Location Grows Revenue for MDM Providers

Advanced location technology expands MDM providers' feature sets and generates new revenue as add-ons to existing offerings. New functionality created by hybrid location can help further up-sell customers on the added security options precise location brings. MDM providers are able to charge a premium for the increasing levels of precision in their device positioning.

This added layer of data gives companies more certainty in knowing their information is protected, and serves to further differentiate MDM providers from the competition. Even without requiring additional hardware, MDM providers can better preserve valuable information and safely track devices using hybrid location.

Hybrid location can guarantee a confidence score for accurate location by combining and comparing different location sources. If one of the location sources has a bad confidence score and does not match up to the other sources, the MDM provider will be notified and can enable the company to remotely lock or wipe sensitive data.

Chapter 2

Integration is a Mindset

CHAPTER 2
INTEGRATION IS A MINDSET

TMDM technology is installed at the device level, so MDM providers are in the unique position to collect proprietary data on usage and employee behavior. MDM providers should consider opportunities to leverage the data they own to attract third party developers, even if they don't use all location data as part of their core experience. By offering device-level location data through an API, MDM providers empower third party developers to build better business apps that integrate with MDM platforms. This will lead to a value-added ecosystem of apps that are available for MDM clients. Supplying this data allows them to extend their SDK, offering the visibility of location based policies into third party apps.

For example, a law firm wants to use a new desktop app to automate timesheets by billing clients based on their time on site. The timesheet company developing the app can create more value for the law firm by leveraging the unique data only an MDM provider has. If an MDM provider opens its API to third party developers, the timesheet app can offer added value by tapping into the MDM's location data. Rather than prompting the law firm's employees to enter their time spent on site with a client, the timesheet app can use MDM data to auto-populate it. This integration makes for a more frictionless user experience for the law firm and its employees, raising the value of the timesheet app and the MDM provider.

By offering device-level location data through an API, MDM providers empower third party developers to build better business apps that integrate with MDM platforms.

Integration with the larger enterprise app ecosystem is important not only for third party developers, but for clients who see integration as a high priority as they grow and scale their operations through other technology platforms. Integration should be core to the MDM mindset in 2014, as it will be a central factor in IT management's purchasing decisions. Enabling developers to add device-level location to their non-mobile apps incentivizes them to create applications that supplement MDM offerings.

Chandra Sekar, Senior Director of Citrix XenMobile says, "Third party developers play a huge role in the MDM industry. Employees are bringing a staggering number of mobile apps into the enterprise on a daily basis. If not managed, these apps can pose a risk to corporate information and corporate networks. Enterprise IT must find a way to mitigate the risk, while enabling employees to take advantage of the powerful benefits mobile apps provide".

Citrix Worx App Gallery

CITRIX® XenMobile

"Employees are bringing a staggering number of mobile apps into the enterprise on a daily basis. If not managed, these apps can pose a risk to corporate information and corporate networks."

Chandra Sekar
Senior Director
Citrix XenMobile

Citrix recognized the need to embrace third party developers, and launched the Citrix Ready Worx App Gallery last August.

An emerging critical factor in how IT decision makers choose MDM solutions is the degree to which MDM software integrates with other technology platforms they want to use. Providers should be aware that because their technology is installed on essentially all of a customers' devices, they have access to proprietary and valuable data. Even if that data--including location--is not core to the MDM providers' experience, third party developers will find it valuable.

Chapter 3

Scaling Secure Data at Secure Locations

CHAPTER 3
SCALING SECURE DATA AT SECURE LOCATIONS

Companies want to be able to control who has access to what data based on where they are - even when offline. Now, they don't have to wait for a device to come online to act on its location and determine whether access to secure data should be granted. Even when a device is asleep in a power saving mode or when apps are running in the background, MDM providers can determine when a device leaves a secure location with geofencing.

Geofencing plays a significant role in the MDM industry, as it allows IT administrators to set geographic boundaries indicating secure areas. Geofencing gives MDM clients granular control over their employee's devices, while respecting their privacy when outside of the office.

Use Case: Geofencing for Improved Security

Geofences can trigger real-time alerts that notify a school administrator when a school-owned device enters or exits an area. This feature would be valuable to educational institutions that want to protect their investment in new technology by ensuring that students do not take devices home, or that they return them on time.

In addition to device security, geofencing can also power document security. This is especially important for securing patient medical records and information. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) established a national set of security standards for the protection of any health information that is stored or transferred in electronic form. HIPAA addresses the technical safeguards that organizations must put in place to secure individuals' "electronic protected health information" (e-PHI).

Today, medical providers are adopting the use of mobile devices to view and share medical documents and data such as computerized prescription entries or electronic health records. Health plans are now enabling access to claims and care management through mobile devices and computers, as well as through member self-service apps. While this means that the medical workforce can be more mobile and efficient and physicians can check hospital records from wherever they are, the rise in the adoption rate of these technologies increases potential security risks.

A major goal of HIPAA is to protect the privacy of individuals' health information while allowing the medical industry to improve the quality and efficiency of patient care by adopting new technologies. MDM providers with precise location abilities can help secure medical records and data by ensuring the proper access to this information.

For instance, a hospital may want to grant its doctors access to patient records only inside hospital walls and in the security of their homes. With MDM, hospitals can geofence not only their property but any location they deem secure.

While geofencing has the capability to improve device and document security, standard geofence offerings are limited. The number of active geofences allowed per Android device caps at 100 and iOS devices at 20. They also limit the shape of geofence boundaries to point and radius. Thinking about creating geofences is easy, but designing, coding and implementing them to get around device limits and be flexibly managed is time-consuming and difficult.

Skyhook's Context Accelerator SDK allows MDM providers to activate an infinite number of geofences regardless of device limitations. Our custom polygon geofences classified by venue type make geofencing thrive at scale without draining device batteries or requiring intensive coding. MDM providers can bring these features into their platforms so clients can manage geofences in the same place they manage the rest of their device settings.

SOURCES:

* ***Gartner:*** *Magic Quadrant for Mobile Device Management Software*
** ***Gartner:*** *Mobile device management tech set to take off*
*** ***Cisco:*** *Data Leakage Worldwide: Common Risks and Mistakes Employees Make*

SKYHOOK®

CONCLUSION

Location services can accelerate the growth of MDM in 2014. Secure BYOD programs that are cross-platform and can integrate with third party apps will stand out in the industry. Customers will look for solutions that can scale with their business, remain cognizant of employee privacy, minimize risk and are easy to implement. In this regard, Skyhook's location will enable the growth of MDM as the new IT standard.

Skyhook's SDK ports easily to any operating system or platform on all smartphones, tablets, and laptops, allowing for the ultimate freedom for BYOD programs. Our technology fields billions of location transactions per month, and intelligently improves with each location request.

YOU MAY ALSO BE INTERESTED IN:

Mobile Device Management Datasheet

Skyhook is the worldwide leader in location positioning, context and intelligence. In 2003, Skyhook pioneered the development of the Wi-Fi Positioning System to provide precise and reliable location results in urban areas. Today, Skyhook's Precision Location provides positioning to tens of millions of consumer mobile devices and applications.

FOR MORE INFORMATION, VISIT: **WWW.SKYHOOKWIRELESS.COM**