The ultimate guide to unified endpoint management (UEM)

Best practices to enable today's digital workplace

mobileiron

490 East Middlefield Road
Mountain View, CA 94043 USA
Tel. +1.650.919.8100 | Fax +1.650.919.8006 -
info@mobileiron.com

MKT-EN-0119-US v6.2

Table of Contents

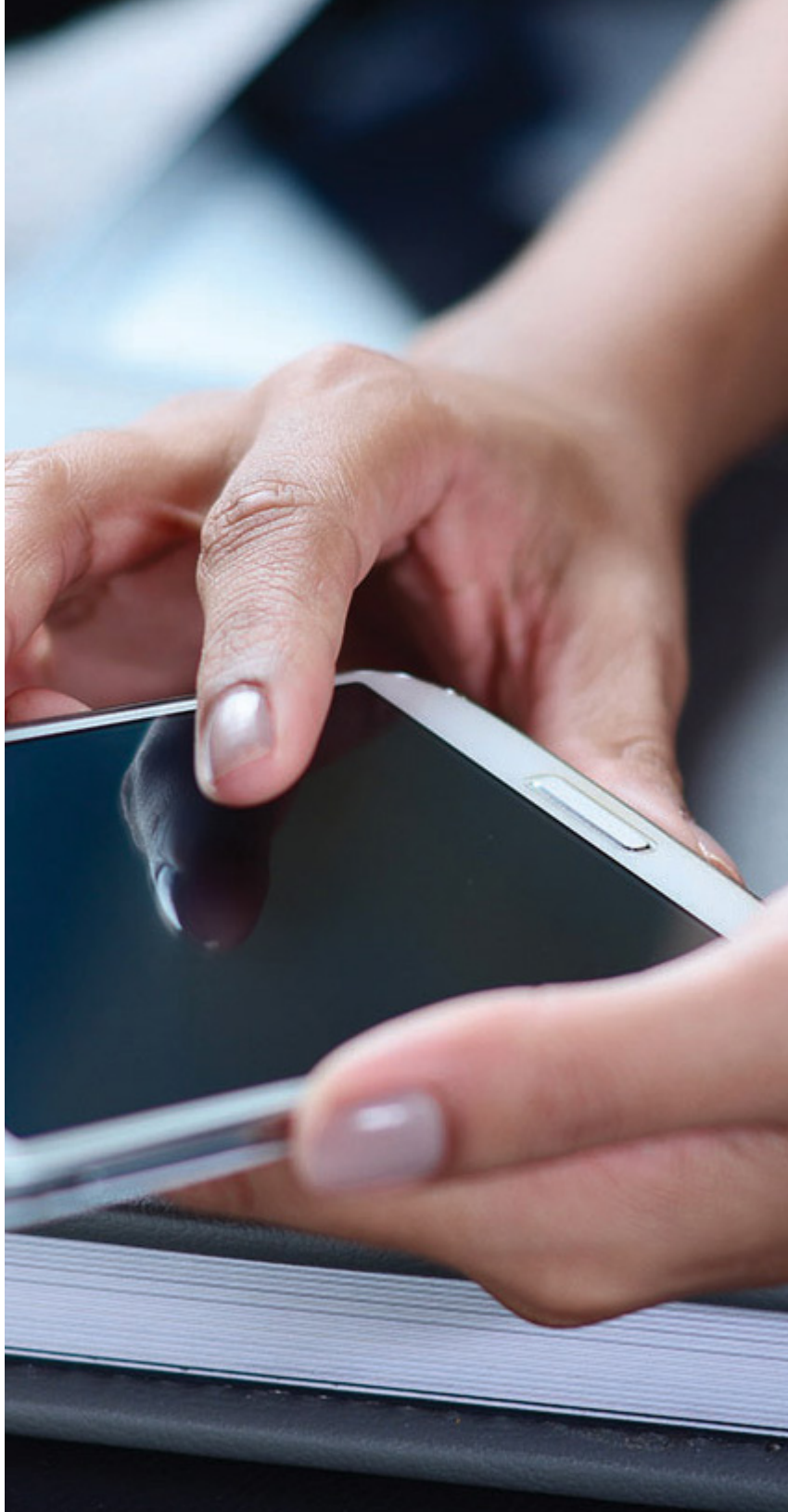
Executive summary

New mobile and cloud computing technologies are changing the digital workplace by empowering users to be more productive, on any device, wherever they work. With so many users, endpoints, operating systems, apps, and cloud services to choose from, today's workers expect instant access to the content they need, and they don't want to jump through a bunch of security obstacles to gain access.

With so much data flowing freely across and outside of the perimeter-less enterprise, IT needs to think about how to establish trust in a zero-trust world where every user, device, app, network, and cloud could potentially be compromised. Building a zero-trust security environment requires a new mindset and technical approach to security. But, like almost everything else in security, starting with good hygiene and establishing a foundational process and architecture are the most important steps. Fortunately, that's something every organization can start doing today.

Unified endpoint management (UEM) plays a critical role in helping organizations transition from traditional enterprise security by establishing a zero-trust environment where users can confidently embrace modern endpoints, desktops, apps, and cloud services for work. UEM provides the foundation for a Mobile-centric security platform with a zero trust enterprise journey that leverages a sophisticated trust model and dynamic policy framework to continuously determine whether to provide access to corporate data. The ultimate goal is to ensure users stay productive and happy on their device of choice, wherever they work, while protecting your business from the latest threats.

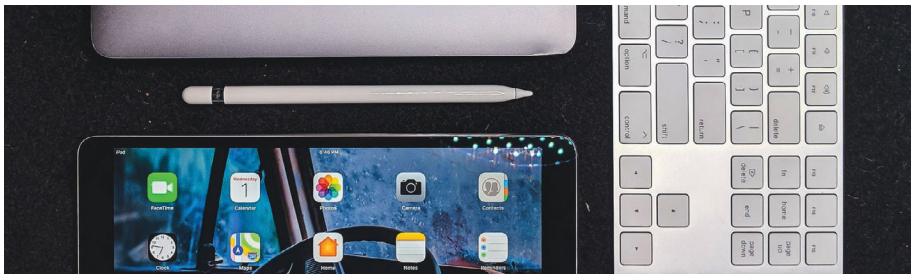
This guide is designed to help mobile enterprise leaders execute a UEM strategy that enables them to transform business processes from legacy systems to secure, modern computing architectures capable of supporting today's digital workplace. In addition to describing how UEM works, this guide also illustrates a typical UEM implementation with detailed, best-practice deployment processes and recommendations for a successful mobile-cloud journey.



Introduction

For decades, the IT-controlled desktop was the main productivity tool in the enterprise. Today, mobile workers no longer want to be tethered to locked-down PC workstations, and they expect IT to support the mobile devices and apps they need to stay productive wherever they work. The rapid transition from client/server computing to mobile and cloud computing has left many IT organizations scrambling to maintain secure control over enterprise data — all without frustrating users who expect complete mobile freedom and seamless access anytime, anywhere.

Compounding this challenge is the fact that mobile and cloud infrastructures are highly decentralized across the perimeter-less enterprise. Organizations might not own all of the endpoints that access enterprise apps and data. For example, they can be owned by employees in a bring your own device (BYOD) scenario. Even devices issued by the organization to its employees fall into a variety of deployment models, such as corporate-owned, personally enabled (COPE) and company-owned, business-only (COBO) devices, and are subject to varying levels of control by the organization. However, even if IT owns the physical device, the device manufacturer controls OS updates and security patches and the user decides when to install them — without any IT intervention. Furthermore, mobile users are now accustomed to going to the Apple App Store or Google Play to download applications instead of waiting for IT to administer them.



"As a CISO, you are up against a growing threat landscape, a shortage of skilled cybersecurity professionals, and non-technical employees who lack awareness of cybersecurity best practices. [1]

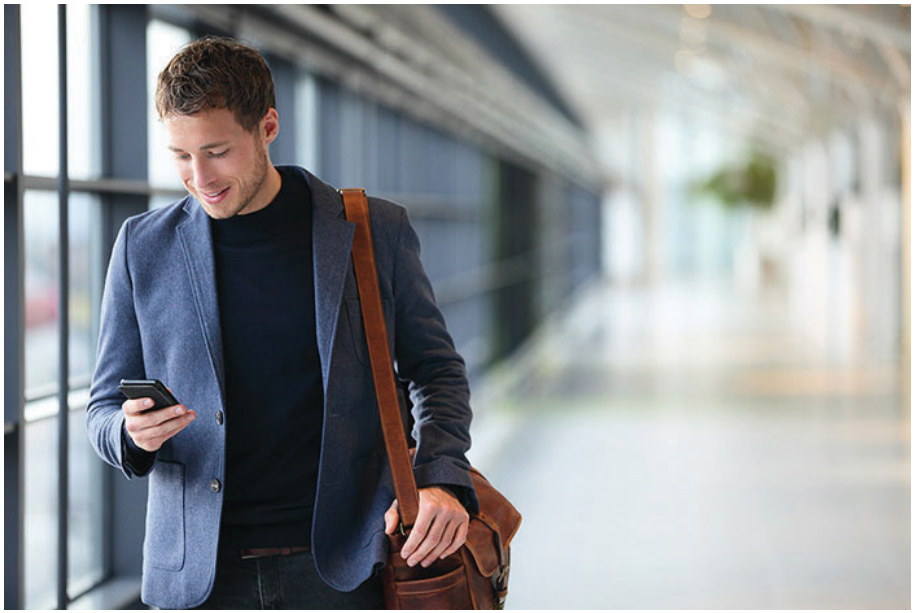
As mobile devices and cloud adoption become more mainstream, IT needs insight into security threats and vulnerabilities on devices and networks they may not own. With the proliferation of mobile threats and network attacks, every IT organization will likely have to manage a security breach such as a malware attack, compromised credentials, or a stolen device — and the ability to respond quickly and decisively is critical. At the same time, CIOs and CISOs need to ensure compliance with government regulations such as the General Data Protection Regulation (GDPR) in Europe, the Health Insurance Portability and Accountability Act (HIPAA) in the US, and the the Payment Card Industry Data Security Standard (PCI DSS), which is a set of security standards designed to ensure secure credit card transactions.

With the era of perimeter-based, IT-controlled desktop security giving way to the modern digital workplace, now is the time for enterprise leaders to learn how UEM provides a secure foundation based on zero trust to ensure complete mobile security without sacrificing mobile productivity.

1 https://www.csoonline.com/article/3244248/data-protection/top-5-cybersecurity-questions-for-the-ciso-in-2018.html

Mobile-cloud security: Know the challenges

Every organization's mobile-cloud deployment strategy will be unique based on their individual business and technology requirements. Yet, many of the challenges are the same for any company. For instance, each organization has to figure out how to support device choice, securely administer mobile apps and content, protect data from an expanding threat landscape, and above all, provide an excellent device experience to end users.



Supporting device choice

The digital workplace is dramatically shifting the role of IT in the enterprise. Instead of dictating which technologies employees will use, IT now needs to support the variety of mobile technologies employees bring into the enterprise. IT organizations that don't support mobile users or their preferred devices will quickly find themselves marginalized because mobile employees can simply go around unresponsive IT organizations.

Mobile app and content management

According to IDC, total mobile app downloads will exceed 210 billion and generate nearly $57 billion by 2020.[2] What does that mean for your enterprise? The demand for mobile apps is exploding, and mobile workers now expect to have more than just corporate email on their devices. And, as more platforms such as iOS increase support for enterprise app development, the demand will only increase. To meet this demand, enterprises can no longer take the approach of first developing for a PC-based world and then transitioning to mobile. All app and content development going forward must be enabled for mobile first.

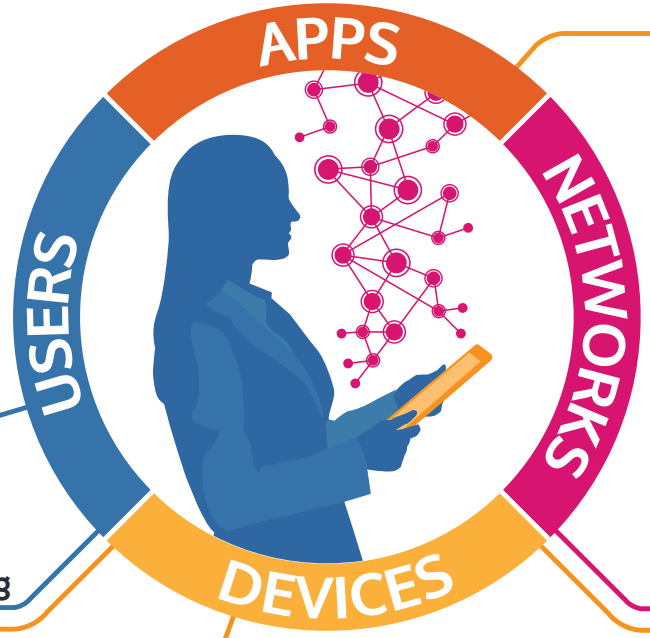
New security challenges

One of the biggest mobile challenges is how to secure data and apps (including third-party apps) on all mobile devices without impacting the native user experience. Before the mobile era, the biggest security risks were malware and viruses due to the vulnerability of open file systems and an unprotected kernel. Today, mobile operating systems have a sandboxed file system and protected kernel, so traditional security threats present less of a concern. However, mobile technologies are exposed to a growing landscape of other types of threats, including user-based, device-based, application-based, and network-based threats.

2 https://www.idc.com/getdoc.jsp?containerId=prUS41240816

Threat vectors

Sandboxed mobile operating systems are secure. Threats such as malware are mitigated by OS design. Preventing data loss on mobile requires focus on a different set of risk vectors.



Malicious or risky apps

Collect and share data such as personally identifiable information (PII) and device location with third-party advertising and analytics systems.

Data loss

Data can be lost through cloud services and productivity apps via open-in, copy, paste, and forwarding functions.

Device tampering

Exploit OS vulnerabilities to jailbreak or root devices, bypass security, and install malicious apps from unauthorized app stores.

Form factor

Portable form factors make mobile devices susceptible to loss or theft.

Always-on connectivity

Mobile devices are hyper-connected and often access sensitive data over untrusted networks, increasing the risk of data loss through Wi-Fi sniffing, rogue access points, and man-in-the-middle attacks.

Unified endpoint management: What is it?

According to Gartner, unified endpoint management (UEM) tools combine the management of multiple endpoint types in a single console. UEM is a comprehensive solution for managing modern mobile devices, desktops, applications, and content across the perimeter-less enterprise. UEM solutions are designed to help companies leverage modern operating systems and mobile technology as tools for business transformation through a zero-trust approach that ensures only authorized users, endpoints, apps, clouds, and networks can access enterprise resources.

UEM tools perform the following functions:

- Configure, manage, and monitor iOS, macOS, Android, and Windows 10. They can also manage wearable endpoints.
- Unify the application of configurations, management profiles, device compliance, and data protection.
- Provide a single view of multi-device users, which helps provide more efficient end-user support and detailed workplace analytics.
- Act as a coordination point to orchestrate the activities of related endpoint technologies such as identity services and security infrastructure.

Benefits of UEM

UEM is designed to help your business transform critical operations with secure mobile and cloud computing that gives IT the control it needs to protect data, and a user experience employees need to stay productive.

Organizational and user control

Establish mobile security protocols that protect your devices, apps, and data without compromising the user experience. With UEM, you can scale to add new features over time as your business needs and budget requirements change.

- **Separate personal and corporate data** on mobile devices and desktops to ensure user privacy while protecting corporate data.
- **Administer an enterprise app storefront** to give employees secure and convenient access to corporate-managed apps.
- **Implement layered security controls** that protect mobile devices and data without impacting the user experience.
- **Selectively wipe enterprise data** from mobile devices and desktops while leaving personal data intact.
- **Enable self-service** so users can enroll and register devices, check compliance, troubleshoot problems, and handle other basic device management issues.

Freedom of choice

UEM is OS- and device-agnostic, which allows users to choose their preferred devices, whether corporate-owned or BYOD, to stay productive wherever they work. IT admins can also deploy either a cloud or on-prem deployment model depending on their business needs.

- **Enable a multi-OS environment** to support iOS, macOS, Android, or Windows 10 devices.
- **Allow users to quickly access enterprise resources** such as corporate email, calendar, and cloud services including Office 365, G Suite, Dropbox, Box, SharePoint, and more.

Experience-driven adoption

The best way to ensure fast, widespread UEM adoption is to make the user experience as seamless as possible. When employees experience a familiar, native device and app experience with enterprise tools, they are more likely to accept compliance measures, avoid shadow IT maneuvers, and stay productive.

- **Provide seamless and instant authentication** with passwordless multifactor authentication (MFA) that eliminates passwords.
- **Enable users to easily access, annotate, and share documents** from email, SharePoint, and other enterprise content management systems and cloud services.
- **Support multi-user profiles** to allow several employees to share a single device.
- **Help users easily maintain compliance** with corporate policies by helping them quickly remediate issues on the device.

Secure business resiliency

Enable workforce productivity with invisible and automated security that protects data integrity, simplifies compliance, and reduces the risk of mobile threats.

- **Deliver immediate, automatic, on-device mobile threat protection** that instantly detects and remediates device threats including phishing attacks
- **Administer certificate-based identity management** to ensure that only authorized users can access the device.
- **Support app containerization** to ensure data within each app is encrypted, protected from unauthorized access, and removed from the device without harming private data.
- **Deploy per-app VPN technology** to limit corporate network access to authorized apps only.
- C**onfigure DLP policies** to prevent data loss through unauthorized file sharing or copy-paste actions.
- **Enforce conditional access** to automatically trigger actions such as compliance notifications or device quarantine whenever devices fall out of compliance.
- **Encrypt email attachments** to ensure they can only be viewed using authorized applications.

Priorities for a successful UEM strategy

Put the user experience first

The user experience must be at the center of any mobility initiative. If the device, app, or content is not something users want or can easily access, then it simply won't be adopted no matter how much the IT organization pushes it. So any UEM platform must be able to support the user experience in the following ways:

Enable choice of device and OS

IT must implement a multi-OS UEM solution that supports modern operating systems such as iOS, macOS, Android, and Windows 10.

Separate personal and work apps and data

Instead of requiring employees to have separate devices for personal and business use, IT should be able to separate business and personal apps and data on a single device (with the possible exception of corporate-owned kiosk devices). This not only simplifies app management, it also protects the privacy of a user's personal data on the device. So if the employee leaves the company, IT can wipe all business resources from the device while leaving personal apps and content intact.

Protect the native device experience

Perhaps most importantly, the device and app management features of the UEM solution should be seamless to the end user. The digital workplace should enable workers to quickly authenticate and access corporate apps and data without entering a username and password every time. Users should also have access to self-service tools that help them manage basic device functions and troubleshoot problems without having to submit a help-desk ticket.

Simplify IT management

The ability to administer and secure a multi-OS environment that includes a range of mobile devices, desktops, apps, cloud services, and content is no small task. For this reason, every UEM solution should enable IT to:

Simplify access control and authentication

Protecting sensitive business data requires IT to ensure that only trusted users and devices can access mobile and cloud enterprise apps. However, username/password authentication can be tedious, frustrating, and insecure on mobile devices. Therefore, the UEM solution should allow users to authenticate quickly through more modern capabilities such as passwordless multifactor authentication.

Support critical business processes on mobile

Employees in the digital workplace need to have essential data at their fingertips to make core business decisions every day. For example, in a retail environment, sales associates can use mobile apps to assist customers throughout the store. They can look up inventory or complete customer purchases, which eliminates long lines at cash registers. A UEM solution should make it easy to deploy business apps to specific users or groups of users through an enterprise app store.

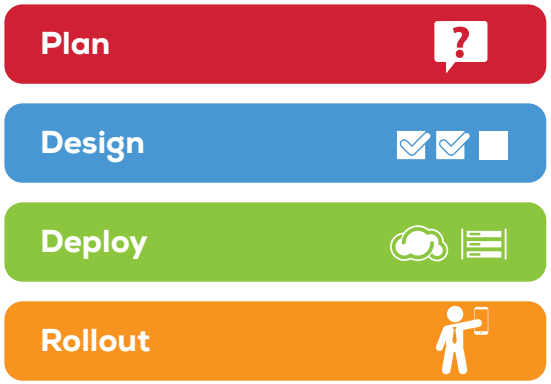
The UEM implementation journey

Most organizations begin their enterprise mobility journey by first providing basic productivity capabilities such as company email and calendar to end users. This helps gain employee trust, which is essential to ensuring success on the rest of the UEM journey. However, the true benefits of UEM happen when organizations enable mobile-cloud computing to become a catalyst for real business transformation.

A layered security approach is fundamental to this transformation because in the mobile-cloud model, perimeter-based security is no longer adequate. Layered security provides multiple types of security across mobile devices, apps, and networks, which helps protect data-at-rest on the device as well as in apps and cloud storage. Best of all, layered security measures operate behind the scenes and remain invisible to the end user, so mobile productivity is never interrupted by security operations.

UEM deployment best practices

UEM deployment typically follows this four-step process:



Phase I: Plan

To begin the planning process, it's important to first know what success means for your organization, and how quickly you expect to achieve it. Gathering feedback from key stakeholders across your enterprise will be critical in the planning stage. For example, some companies define success as a fairly straightforward deployment that provisions security policies, email, and Wi-Fi profiles to users. In a basic deployment, device registration is handled largely by IT staff who are familiar with mobile operating systems and their features. Companies that plan to go beyond a basic UEM deployment will need to address the following questions in the planning stage:

1. Are your employees experienced with mobile devices and modern operating systems?

Technically savvy users will be more self-sufficient than those who are new to mobile. Users with less technical experience may require more IT support.

2. Identify your Use Case.

Each deployment is highly dependent upon the end use case and a successful implementation requires a vendor with direct experience. Identify a vendor that supports many use cases including:

Healthcare:

- Shared Devices
- Secure EMR access
- Clinical Communications
- Nurse to Pharmacy Communications
- Secure Consultation

Retail:

- Shared Devices
- Point of Sale Kiosks
- Inventory Management Touchless transactions
- NFC technology and analytics

Manufacturing:

- Devices
- Supply Chain management Inventory control

HealthcareTransportation

- Realtime ticketing
- Baggage control
- Driver management
- Ticketing kiosks
- Asset tracking

3. Which modern operating systems, mobile devices, cloud services, and desktops will your organization support?

The answer to this question requires knowing which devices and clouds are most popular among employees (especially for BYOD) and whether or not they support your business needs and security requirements.

4. How complex is your network infrastructure?

A single data center rollout with an internal set of network services will require fewer resources than a multi-site rollout with complex networking and infrastructure requirements. Outsourcing IT services will require additional planning.

5. How mature is your IT governance framework, policies, and processes?

Effective IT governance ensures on-time, on-budget program development and solution delivery that meets your goals. Organizations that lack an established or mature IT governance program may require more time and staffing resources to implement their UEM solution.

6. How effective are your employee education and training resources?

Companies with existing training and education frameworks and infrastructure can accelerate a UEM rollout and program adoption for both employees and help-desk staff. Building an employee education initiative will require more effort up front, but will pay off with the development of more mobile-savvy workers and fewer help desk calls.

7. Does your IT team have experience with certificate authentication?

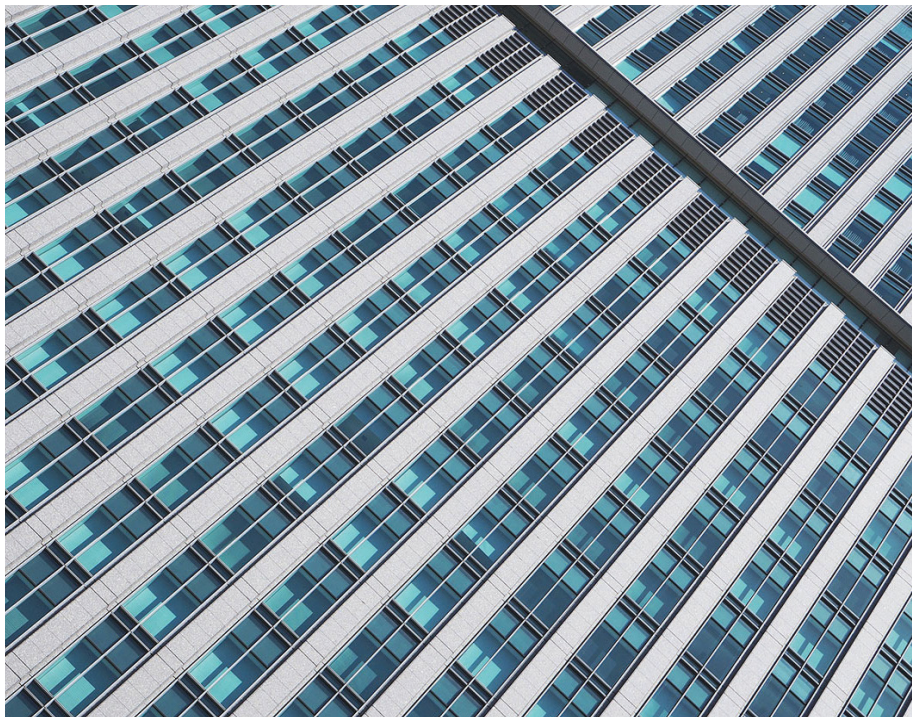
Certificate authentication is an essential security capability in mobile initiatives. Having internal expertise in this area will help accelerate the deployment and setup process.

8. Can your IT organization develop and deploy mobile enterprise apps?

Anyone who develops apps for your company should have the experience and know-how to deliver an outstanding mobile user experience. This will be critical to ensuring the success of your mobile strategy. If you don't have skilled app developers in-house, you will need to outsource this key function.

9. What are your company's security requirements?

Information protection and data security on mobile devices are critical components of any UEM deployment. Companies in highly regulated industries will likely have a lower tolerance for risk (and therefore more security requirements) than companies with a higher risk tolerance.



Phase II: Design

This phase of UEM deployment is all about designing the policies that govern your mobility strategy.

1. Define roles

First, determine how you want to organize administrative tasks like help-desk support, user registration, and device configuration management. For example, how many levels of help-desk support do you need? Who will develop and manage your in-house apps — existing staff or third-party developers? Who will oversee policy and configuration processes?

2. Define visibility

Second, you will need to determine which users and devices each IT admin will manage and how much control and visibility they will have. Also, your device and user management policies may vary according to business unit or geographical region. For instance, some regions have different privacy regulations, such as GDPR in the EU and HIPAA in the US. Your security policies will need to ensure mobile employees in those regions can meet compliance standards.

3. Assign actions

Third, assign management tasks to each IT role in your organization. For instance, which administrators will manage the distribution of apps, policies, and configurations based on your visibility policies?

4. Manage distribution

In this final step, decide which apps, policies, and configurations will be deployed, as well as who deploys them and when. Identify which IT admins will be responsible for various distribution roles, and prevent admins from performing any unauthorized actions.

1 Define roles	2 Define visibility	3 Assign actions	4 Manage distribution
How many admins? What responsibilities?	*Which users/devices does each admin view and report on?*	*Which actions can each admin perform?*	*Which apps, policies, and configurations can each admin distribute to users and devices?*

Phase III: Deploy

In the deployment phase of your UEM initiative, you will need to choose whether to deploy your platform as an on-prem or cloud-based solution.

Option 1: On-premises solution

An on-prem solution is packaged as an easy-to-install software appliance that plugs into the corporate network and can be up and running in less than a day.

Option 2: Cloud-based solution

A cloud-based UEM deployment integrates tightly with enterprise messaging and security systems, such as corporate email and corporate directories. Cloud-based deployment options are typically offered on a subscription basis.

Phase IV: Rollout

Once your UEM solution is ready for rollout, you will need to make sure your help-desk admins are thoroughly prepared by enabling them to:

- Understand the multi-OS management issues they are likely to face. Clearly define the troubleshooting steps, escalation process, and responsibilities for resolving each type of device, app, server, or network issue.
- Engage device experts to provide deeper insight into all of the devices your help-desk staff will encounter.
- Access the resources they need for the level of support they will be delivering.
- Ensure they have easy-to-use troubleshooting resources, such as problem resolution scripts and an online knowledge base.
- Leverage ongoing education opportunities to ensure they stay up to date on mobile device upgrades, infrastructure updates, and more.

How to choose a UEM solution provider

One of the most frequently asked questions about UEM is how to find a provider that can meet all of your unique requirements. Here are a few key criteria that can help narrow and accelerate your search:

Choice computing and end user experience

Think about what mobile devices looked like five or 10 years ago. Some of those brands barely exist anymore. Chances are, mobile technology will look very different five years from now, especially as more devices continue to proliferate. Instead of trying to predict which mobile platforms will rise to the top in a hyper-competitive market. The ability to provide a seamless and delightful end user experience during device onboarding helps improve user productivity. It's much easier to adopt a solution that allows users to choose devices that best support their productivity and success. Then there's no need to worry about which mobile devices and desktops to support, because the vendor will be able to manage them all.

Purpose-built mobile-centric security platform

Mobile-cloud computing has rapidly emerged as the next dominant enterprise computing model. To support this model, it's critical to find a vendor whose mobile-centric security platform can grow with you as your business needs evolve. And this means looking for a solution that has been built from the ground up to secure and manage the diverse modern operating systems and enable massive scalability. UEM solutions that are simply add-ons or a component of an existing infrastructure may not be comprehensive or integrated enough to deliver the scalability and reliability growing enterprises need.

Extensive partner ecosystem

In addition to choosing a vendor with a strong vision and purpose-built UEM platform, a solution provider should also maintain a diverse ecosystem of best-of-breed solution providers. This ensures access to a broad range of technology solutions to meet current business and infrastructure requirements.

Reputation for customer success

Review the UEM vendor's customer portfolio and standing within the analyst community. Not only should the vendor serve a diverse, global customer base, it should have a UEM leadership ranking, customer reviews and awards. By researching these factors you can be sure the vendor has the proven longevity, experience, and credibility necessary to meet your long-term mobility goals.

Choice of Deployment Options:

Organizations have different data protection requirements for mobile and desktop devices. Some may choose to keep their data on-premises because of mandatory compliance requirements as well as in-house IT staff while others may have the flexibility to store their data in the cloud. There are some organizations that might choose a combination of both for their geographically distributed locations. Look for a vendor that offers a choice of deployment options options

Summary

Enterprise mobility is not just about buying the latest mobile devices or putting email on an employee's phone. It's about transforming your business through a mobile-centric security platform with a zero trust model of security that ensures compliance while giving your users the freedom they need to be productive and successful wherever they work. Although embarking on a mobility initiative can seem like exploring vast, uncharted territory, the right UEM solution can help you quickly move forward on your journey to becoming a modern mobile enterprise.

About MobileIron

MobileIron is redefining enterprise security with the industry's first mobile-centric security platform for the Everywhere Enterprise. In the Everywhere Enterprise, corporate data flows freely across devices and servers in the cloud, empowering workers to be productive anywhere they need to work. To secure access and protect data across this perimeter-less enterprise, MobileIron leverages a zero trust approach, which assumes bad actors are already in the network and secure access is determined by a "never trust, always verify" model.

MobileIron's platform combines award-winning and industry-leading unified endpoint management (UEM) capabilities with passwordless MFA (Zero Sign-On) and mobile threat defense (MTD) to validate the device, establish user context, verify the network, and detect and remediate threats to ensure that only authorized users, devices, apps, and services can access business resources in a "work from everywhere" world. Over 20,000 organizations, including the world's largest financial institutions, intelligence agencies, and other highly regulated companies, have chosen MobileIron to enable a seamless and secure user experience in the Everywhere Enterprise

Take the next step

Find out how MobileIron can help you securely transform your critical business processes with our proven, industry-leading UEM platform and professional services. Please visit us at www.mobileiron.com