



The Ultimate Guide to Unified Endpoint Management (UEM)

Best practices to make the Everywhere Workplace possible

Table of Contents

Executive summary	3	The UEM implementation journey	9
Introduction	4	UEM deployment best practices	9
Mobile-cloud security: Know the challenges	5	Phase I: Plan	10
Unified endpoint management: What is it?	7	Phase II: Design	12
UEM capabilities	7	Phase III: Deploy	13
Benefits of UEM	7	Phase IV: Rollout	13
Priorities for a successful UEM strategy	8	How to choose a UEM solution provider	14
Put the user experience first Simplify IT management	8	Summary	15

Executive summary

New mobile and cloud computing technologies are making the Everywhere Workplace possible. These technologies empower 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.

The Everywhere Workplace makes business more flexible, and it also means more data flowing freely across and outside of the perimeterless enterprise. That's why IT needs to establish trust in a zero trust world. While it's true that a zero trust world means every user, device, app, network and cloud is at risk of compromise, this isn't a reason to resist progress. Instead, it's a reason to do it right. Building a zero trust security environment requires a new mindset and technical approach to security. Like almost everything else in security, this has to start with good hygiene and a foundational process and. 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 to a security landscape that's compatible with the Everywhere Workplace. UEM establishes a zero trust environment where users can confidently embrace modern endpoints, desktops, apps and cloud services for work. UEM leverages the trust model and policy framework needed to continuously determine whether to provide access to corporate data.

The ultimate goal: ensure that 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 the Everywhere Workplace. In addition to describing how UEM works, this guide 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 perimeterless 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. All are subject to varying levels of control by the organization. And 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 Store to download applications instead of waiting for IT to administer them.

As much as some want to frame this up as a recipe for disaster, it doesn't have to be. It's simply a reality of the shifting landscape, and that means making shifts along with it. Or, better yet, making shifts to stay ahead of it.

“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 even 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. These may include a malware attack, compromised credentials or a stolen device. Is this a reason to panic? No, but again, it's a reason to plan. The ability to respond quickly and decisively is critical.



Meanwhile, 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 Payment Card Industry Data Security Standard (PCI DSS), which is a set of security standards designed to ensure secure credit card transactions.

The era of perimeter-based, IT-controlled desktop security is giving way to the Everywhere Workplace. Let's make that a good thing. Now is the time for enterprise leaders to learn how to ensure complete mobile security without sacrificing mobile productivity. With a secure foundation based on zero trust, UEM is how mobile security and mobile productivity coexist.

Mobile-cloud security: What you need to know

There's no one-size-fits-all mobile cloud deployment strategy. Every organization's strategy will be unique based on their individual business and technology requirements. That said, you're not alone. Many of the challenges are the same for any company. Case in point: Each organization must 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.

Here's a snapshot at a few of these common potential challenges:

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 that employees bring into the enterprise. Why be so accommodating? If IT organizations don't support mobile users or their preferred devices, mobile employees can simply go around the organization. Not an ideal scenario.

Mobile app and content management

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

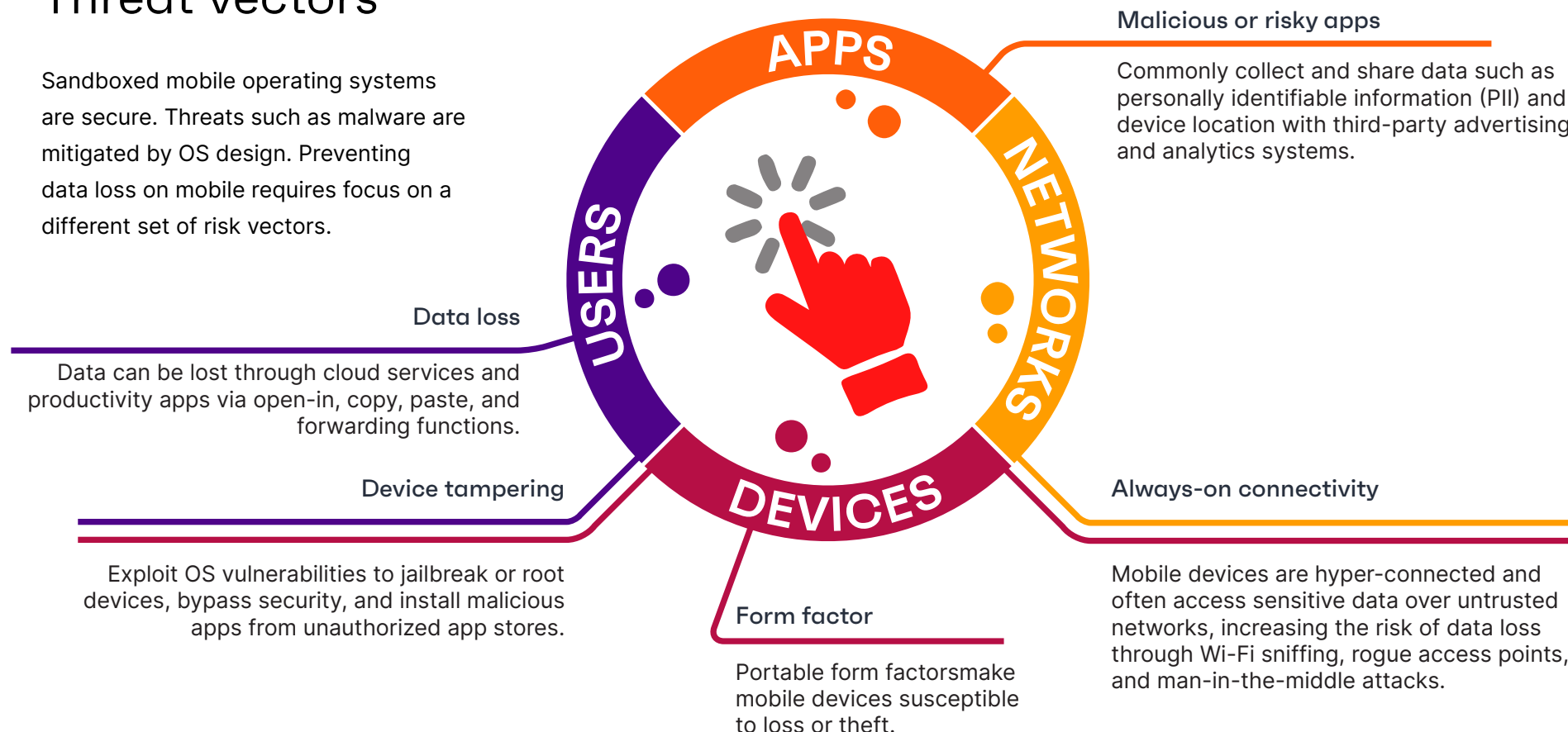
One of the biggest mobile challenges is how to secure data and apps (including third-party apps) on all mobile devices without impacting the native user experience.

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, we've traded one security challenge for a host of others. Mobile technologies are exposed to a growing landscape of threats, including user-based, device-based, application-based and network-based threats.



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.



Unified endpoint management: What is it?

Gartner explains that unified endpoint management (UEM) tools combine the management of multiple endpoint types (devices) in a single console. UEM is a comprehensive solution for managing modern mobile devices, desktops, applications and content across the perimeterless 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 are built for versatility.

Capabilities include:

- Configure, manage, and monitor iOS, macOS, Android and Windows 10. They can also manage wearable endpoints, as well as ruggedized devices often leveraged by frontline workers.
- 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: a) gives IT the control it needs to protect data, and b) delivers the 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. For example:

- 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-premises deployment model depending on their business needs. With UEM, you can:

- 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. More benefits:

- Provide seamless and instant authentication with passwordless multi-factor authentication (MFA).
- 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.
- Promote easy compliance with corporate policies by helping users quickly remediate issues on the device.

Secure business resiliency.

When security is invisible and automated security, your workforce can focus on doing what they do best. (And that means productivity.) This automated security protects data integrity, simplifies compliance and reduces the risk of mobile threats. Here's what that looks like:

- Deliver immediate, automatic, on-device mobile threat protection that instantly detects and remediates device, network, and application-level

threats as well as 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.
- Configure 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 isn't something users want or can easily access, then it simply won't be adopted – no matter how much the IT organization pushes it. That means any UEM platform must be able to support the user experience.

Here's how:

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. That means that 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-servicetools that help them manage basic device functions and troubleshoot problems without having to submit a helpdesk ticket.

Simplify IT management.

IT management for this sort of strategy is no small task. We're talking about the ability to administer and secure a multi-OS environment that includes a range of mobile devices, desktops, apps, cloud services, and content. That's why 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. The problem: 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 like passwordless multi-factor 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. Picture a retail environment, where sales associates can use mobile apps to assist customers throughout the store, looking up inventory to avoid trips to the back room or completing purchases to cut down on 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 end users with basic productivity capabilities like company email and calendar. This helps gain employee trust, which is essential to ensuring success on the rest of the UEM journey. That's a great start, but 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. Why? 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:

Plan



Design



Deploy



Rollout



Phase I: Plan

To begin the planning process, it's important to first know what success means for your organization – plus how quickly you expect to achieve that success.

In the planning stage, take the critical step of gathering feedback from key stakeholders across your enterprise to find out what success looks like. 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. What is the 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 a wide variety of use cases, including:

Healthcare:

- Shared devices
- Secure EMR access
- Clinical communications
- Nurse-to-pharmacy communications
- Secure consultation

Manufacturing:

- Devices
- Supply chain management inventory control

Retail:

- Shared devices
- Point of sale kiosks
- Inventory management touchless transactions
- NFC technology and analytics

Healthcare transportation

- Real-time 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 lacking 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 helpdesk 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?

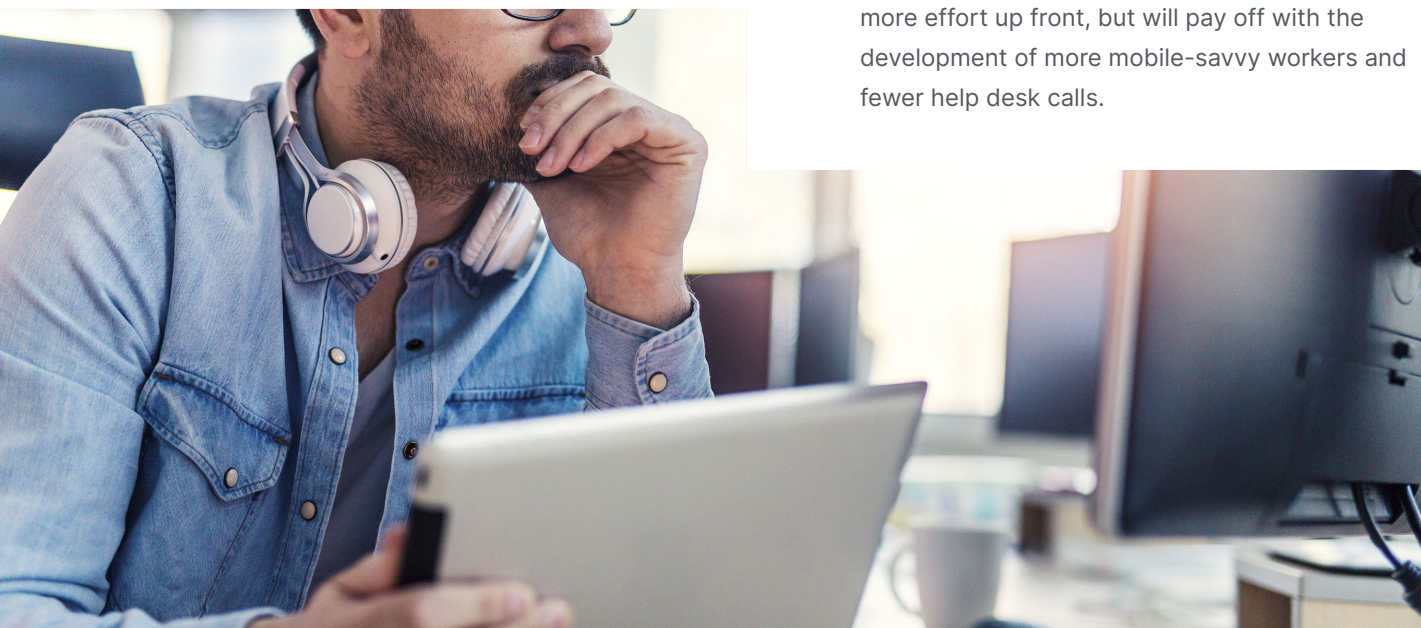
Certificate authentication is an essential security capability in mobile initiatives. Having internal expertise in this area will help accelerate the deployment and setup process.

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'll 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 helpdesk support, user registration, and device configuration management. For example, how many levels of helpdesk 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, determine which users and devices each IT admin will manage, and how much control and visibility they'll have. Keep in mind that your device and user management policies may vary according to business unit or geographical region. For example, some regions have different privacy regulations, such as GDPR in the EU and HIPAA in the U.S. Your security policies will need to ensure that mobile employees in those regions can meet compliance standards.

3. Assign actions.

Third, assign management tasks to each IT role in your organization. Think: 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.



Phase III: Deploy

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

Option 1: On-premises solution

An on-premises 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.

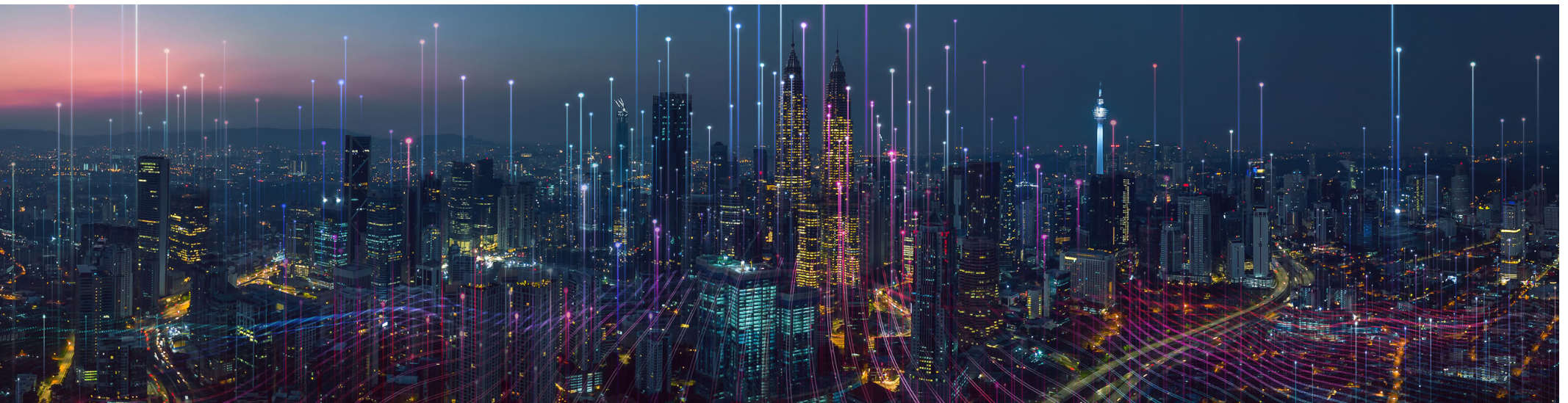
Option 2: Cloud-based solution

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, it's important to make sure your helpdesk admins are thoroughly prepared. This means 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 helpdesk 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 hypercompetitive market, opt for a vendor that allows users to choose devices that best support their productivity and success – and can manage the ever-evolving device landscape, no matter what comes next. When a vendor can manage any device – and provide a seamless and intuitive end user experience during device onboarding – there's no need to worry about which mobile devices and desktops to support.

Purpose-built security platform for the Everywhere Workplace.

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 security platform can grow with you as your business needs evolve. 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.


Summary

Embracing the Everywhere Workplace 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 zero trust security platform that ensures compliance – all while giving your users the freedom they need to be productive and successful, wherever they work.

The Everywhere Workplace is already happening. Rather than scramble to keep up, the right UEM solution can help you quickly and seamlessly navigate this shift so you're ready for what's now and what's next.

About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT networks, applications and data to stay productive as they work from anywhere. The Ivanti automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. More than 40,000 customers, including 78 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work. For more information, visit www.ivanti.com

The Ivanti logo consists of the word "ivanti" in a bold, lowercase, sans-serif font. The "i" is red, and the "vanti" is black. A small registered trademark symbol (®) is located at the top right of the "i".**ivanti®**A vertical bar with a red-to-orange gradient, positioned to the left of the contact information.

ivanti.com
1 800 982 2130
sales@ivanti.com

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

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