Re-imagining your desktop management strategy for a new era of mobility

A Wanstor Guide

wanstor

Contents

wanstor

Introduction

This guide is designed to help IT Managers re-imagine their desktop management strategy for a new era of mobility.
Mobility is reaching a critical tipping point in many business and not for profit organisations.

It only seems yesterday that many organisations were viewing *"mobility"* as an isolated project through which IT could enable email on mobile devices. Now, most see it as a strategic initiative for mobilizing business apps that can impact a range of outcomes.

With this shift in mindset, smart business and not for profit organisations are moving away from tactical point solutions for mobile device and desktop management, and instead are searching for a secure, comprehensive, unified and futureproof *"mobility platform"*.

Enterprise applications, many of them cloud based, are now at the centre of mobile productivity, because mobile workers require access to information anytime, anywhere and from any device.

Traditional security perimeters are shifting as sensitive documents are regularly shared outside the walls of the "organisation". Data may now reside on and move between mobile devices; desktops and laptops; public, private, and even personal clouds.

On the positive side of things these changes offer a clear opportunity to boost productivity and job satisfaction, improve customer engagement, and increase employee productivity.

But in order to take advantage of these benefits, business and not for profit organisations must be ready to overcome the challenges *"mobility"* brings with it.

Whilst yesterday's focus was on MDM, and then EMM, business and not for profit organisations today are seeking solutions for Desktop Management or Unified Endpoint Management, which encompasses management, security and identity across mobile devices as well as desktops, laptops and other endpoints.

As organisations prepare for a growing range of end user and Internet of Things requirements, it's critical that they can maintain visibility and control across their endpoint environments from a unified platform.

At Wanstor we believe organisations of all sizes need to concentrate on developing a mobile strategy first of all before implementing a solution. By taking the time to discuss and develop the right mobility solution, IT teams can expect significant benefits.

The right *"mobility"* solution improves productivity, security, and privacy, while making it easier for IT administrators to manage the growing number of roles, apps, operating systems and device types.

This document will cover many of the key factors to consider as IT Managers form or re-form their mobility strategy. It should be noted that this document should provide a starting point for IT Managers it is not an all-encompassing guide.

There are many factors which will affect a mobility strategy depending on the unique qualities of each organisation.

Though the process can be time-consuming and occasionally political, working out the answers before deciding on a new solution will save time, reduce costs, and prevent headaches every step of the way.

Mobility is a journey, and to begin, it's useful to understand where your organisation falls on the mobile maturity curve. This will help make sure that the solution chosen meets organisational needs today, and in the future.

The Mobile Maturity Curve: Where is your organisation?

To help IT managers on their *"mobility"* journey Wanstor Desktop management experts have developed a Mobile Maturity Curve (See figure 1). There are four general stages to the mobile maturity curve. As your business or not for profit organisation accelerates along the curve, your mobile approach will gradually become more transformative as you adopt new strategies, incorporate new tools, modify existing business processes and eventually create entirely new business models.

At the same time, security requirements increase as more and more corporate applications become mobilized.

The Mobility Maturity Curve Visualised

Must Protect

+ Content
+ Credentials
+ Configurations

Across Pervasive

+ Endpoints
+ Systems
+ Clouds

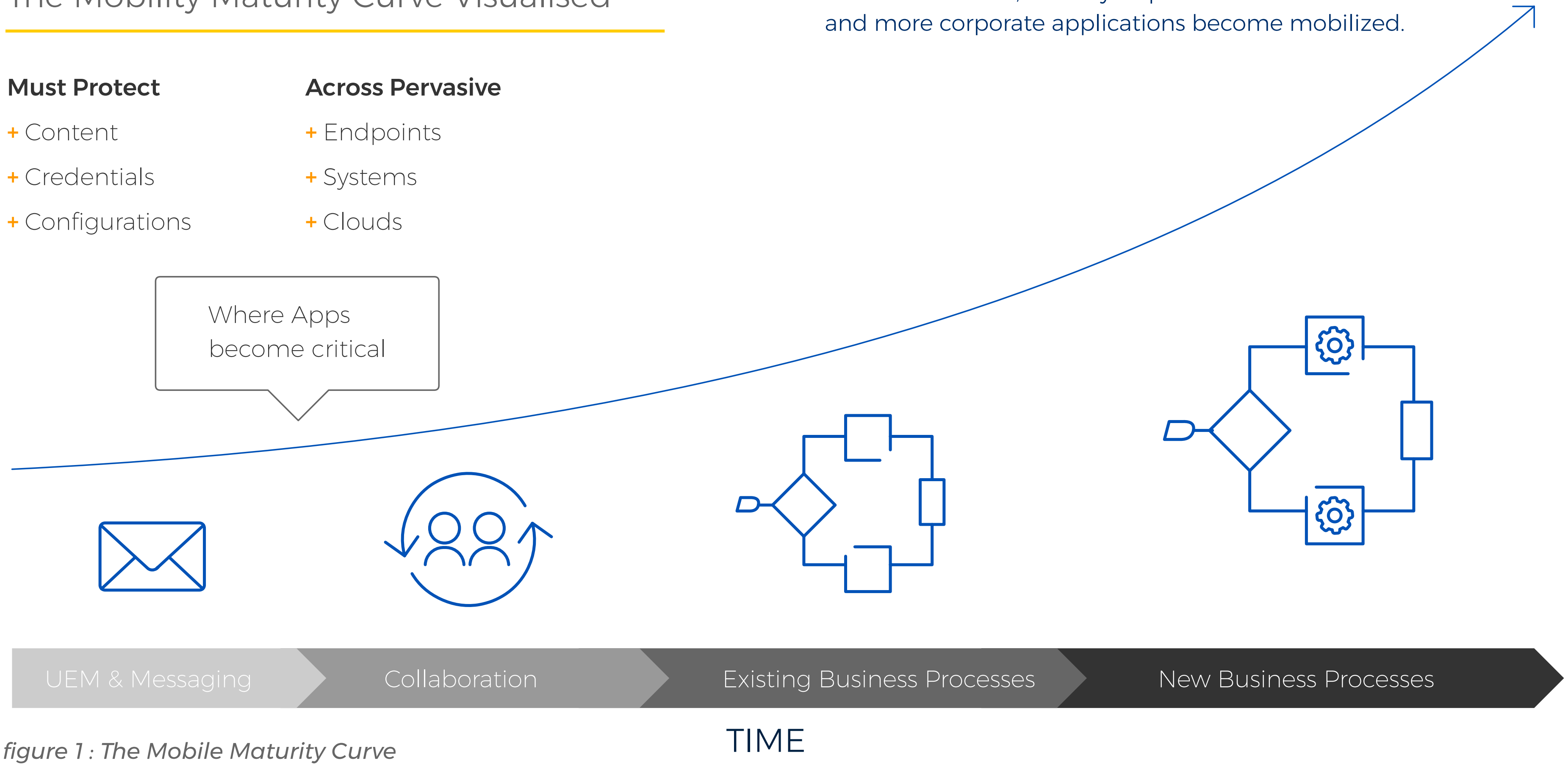


figure 1 : The Mobile Maturity Curve

Why You Need a Mobile Strategy

A mobile strategy is a plan that lists and describes a business or not for profit organisations key requirements and positions on a wide range of mobility issues.

The purpose should be to gather input from all stakeholders to create a strategy that supports the goals of the business without compromising on security or privacy. Without a mobile strategy, making the right decision on a long-term solution can be almost impossible.

Here are some of the key questions IT Managers should be asking key stakeholders in their organisation, depending on their stage in the mobile maturity curve:

- What kinds of mobile apps do we need to roll out to leverage mobility and improve productivity in our organisation?
- How confident are we when it comes to the security of business data - (including that of our customers / clients) in an increasingly mobile and cloud-oriented environment?
- Are we able to accurately forecast IT expenses around mobility? Do we have a solution that can meet our needs today and tomorrow?
- How do we help app owners, app developers, and IT to work together to respect a common security baseline?
- How do we make sure different development teams are able to apply the same security capabilities across all app types?
- How will we address continued growth in users, devices and data as mobile becomes a bigger part of the business?
- How easy is it to meet our compliance or security requirements?
- What advantages could we gain by reducing the number of vendors and solutions in our mobility environment?
- How successfully are we addressing our employees’ trust and privacy issues?

The four stages of the mobility curve: explained

BASIC MOBILITY

Basic endpoint management and email are often the first investments organisations make. Doing so can generate quick productivity gains with limited investment, particularly when coupled with a BYOD initiative. However, managing a diverse mobile fleet can open the organization to new threats.

Challenges at this stage

- Starting to secure basic corporate data (email, attachments) on mobile devices
- Understanding how devices are used
- Establishing technical expertise in-house

Signs your business is at this stage

- Investment in mobility is typically minimal. It's a project, not a company wide initiative
- Mobile app development is not yet on your radar
- You understand that mobility is critical to your business objectives, but aren't sure where to start

MOBILE COLLABORATION

Once an organization's users start getting mobile email and attachments, they naturally want to do more, and the productivity opportunities that mobility offers become harder to ignore. Once a business has made a start with mobility, the next step is to further enable employees through better collaboration and workflow optimization. Most MDM-only platforms lack the necessary tools to secure mobile applications and protect business data.

Challenges in this stage

- Mobilizing the key Microsoft® applications that employees rely on: Exchange, Office 365, SharePoint™, OneDrive for Business, Skype for Business, Dynamics CRM, etc.
- Implementing document workflows with security and control
- Ensuring a positive mobile-user experience
- Protecting employee privacy

Signs your business is at this stage

- Investment in mobility is still minimal to moderate
- You're mobilizing horizontal business apps related to collaboration, such as SharePoint and enterprise instant messaging (EIM)
- You're increasingly concerned about data leakage as more business apps are deployed
- Lines of Business (LOBs) are starting to ask for more role-based, specific applications to improve business outcomes

MOBILIZING EXISTING BUSINESS PROCESSES

By now, teams are used to working together from just about anywhere through the core collaboration and communication tools you've mobilized, and again, decision makers, particularly on the LOB side, will be encouraging IT to go further still.

The next stage of the mobility curve is the large-scale mobilization of an organisations existing business processes and critical applications. Typically, it's during this stage that organisations identify gaps in their app inventory and begin looking into developing their own custom, internal mobile apps.

Challenges in this stage

- Aligning mobile apps and initiatives with existing business processes and identifying gaps to fill with custom projects
- The emergence of new forms of data, or new uses for existing data
- Incorporating mobile applications or application processing into existing infrastructure
- Continuing to adhere to corporate security policy and industry regulations, particularly with regard to customer and other regulated data

Signs your business is at this stage

- Your move to collaboration apps is well-received across your business, and users are demanding more apps to get their jobs done
- You've begun mobilizing existing business processes, or are planning your future mobile investments
- Investment in mobility is moderate
- You've started deploying applications to support priority business roles in your organisation, such as sales, executives, field forces, etc.
- You're planning to start developing internal applications in the near future
- You're identifying gaps to fill with custom apps across devices, operating systems, and clouds
- You've implemented a platform that lets you manage the three Cs of secure mobility: Corporate content, user credentials, and application configurations

EMERGENCE OF NEW BUSINESS PROCESSES

Finally, once you've mobilized existing business processes, the next phase is about business transformation — using mobility for competitive advantage (including cost savings, customer experience improvements, and new revenue opportunities).

This is the point at which your mobile ROI is maximized, and mobility is pervasive throughout your organization. A business typically becomes flooded by mobile applications — often hundreds of them.

Mobile devices become so widespread that managing single devices and applications is highly inefficient and often inconsistent from a security standpoint.

The organisation will have entered into a stage of pervasive mobile computing, whereby corporate data is now on phones, tablets, PCs, and wearables, on back-end systems, clouds, even personal clouds.

Digital Rights Management capabilities (DRM) for file-level security policies are needed to provide security, discovery and containment.

Challenges in this stage

- Managing a large volume of enterprise applications across devices, operating systems and clouds
- Developing a back end to support new mobile applications, business models, and devices
- Leveraging enterprise identity stores and authentication schemes to support single sign on, even to cloud services
- Aligning mobile app development with existing business needs

Signs your business is at this stage

- Your endpoint management solution is part of a larger approach to mobile management
- You're looking for a way to manage data, documents, and roles in addition to applications and devices
- You've begun deploying custom, internal applications
- Investment in mobility is typically moderate to high
- Your organization is being disrupted by new business models and is now maximizing its return on mobility investment

Key Factors in Making a UEM or Desktop Management Platform Decision

Once the IT Manager is able to locate their organisations position on the mobile maturity curve, it's easier to identify the kinds of issues needed to be solved in the near term. The IT Manager should also take a longer term view as well to make sure the solution chosen will support the organisations mobility goals in the future as well. The list that follows is not exhaustive, but will provide IT Managers with an overview of top factors to consider. If your stakeholders can all understand and agree on the importance of these issues, then the IT team will be in a position to decide on which Desktop management platform is an appropriate solution.

- Cross-platform endpoint management
- Mobile application security and management
- Security certifications and credentials
- User privacy protection
- Document control
- Deployment model (cloud or on premises)
- Migration and implementation
- Technical support
- Training and user features
- Pricing and total cost of ownership (TCO)

In the next section of this white paper we will discuss each of the identified areas below on the list in further detail.

Wanstor's Top Mobility Pain Points

- The need for real security across corporate content, application credentials, and device configuration data, and the need to protect against data leakage.
- The need to address both current and evolving business needs such as new applications while integrating Desktop Management with key business systems and processes.
- The need for a security solution that doesn't hinder employees and drive them to find workarounds.
- The rise of cloud computing, and the difficulties associated with securing files across both cloud applications and mobile devices.
- Inconsistent security models across applications due to different development technologies (for native apps, HTML5, hybrid development environments, etc.)
- Scaling of mobile management infrastructure to respond to evolving business needs.
- The difficulties associated with providing mobile tech support
- for an entire enterprise.

CROSS-PLATFORM ENDPOINT MANAGEMENT

Whether the devices are bring your own (BYO) or corporate-owned, managed by your IT department or not, chances are your work environment already involves multiple mobile operating systems and device types.

IT Managers need to make sure the chosen UEM / DM solution can manage those devices in all the ways required, across every use case and role, including business users, remote workers, highly-sensitive users, shared devices, desktop systems and kiosks.

IT managers should consider not only the platforms used today, but those you might want to use in the future, including capabilities such as Android for Work, Samsung Knox Workspace, and iOS Managed Apps.

From a day-to-day management perspective, the platform chosen should allow IT administrators to manage everything - user groups, administrative roles, software configurations, email profiles, IT policies and more - from one unified console.

Given that the IT department is constantly overworked/under resourced in many medium – large organisations they do not require the challenges of learning an entirely new management paradigm, therefore a user-friendly, intuitive interface is critical.

Among other factors to consider the IT Manager needs to understand whether the solution will:

Simplify user setup and enrolment: by allowing users to quickly self enrol over-the-air. Streamlining the enrolment process increases user satisfaction while driving down mobile support costs.

Enable rich policy controls: IT Managers will need the ability to define and deploy all the right policies for their organisation, spanning passwords, device encryption, camera, Wi-Fi, VPN, and more. Should a device be lost, stolen, retired or replaced, the IT Manager will need the ability to wipe business data without impacting personal content or apps.

Support regulatory compliance or high-security requirements

Organisations in regulated industries, such as financial services, healthcare, law, and government, must comply with stipulations governing the security of customer, financial, and other data.

For many organisations, supporting these ever growing mobile security requirements takes up valuable time and energy. Your UEM/DM solution must be compliance-ready by design. The IT Manager should check for a list of security certifications and accreditations to see how solutions address specific needs.

Detect jailbreak / rooting: For end users, rooting or jailbreaking a device can be tempting, as it offers more freedom to customize how their smartphone or tablet functions. At the same time, it represents a considerable security risk, as the process involves disabling an operating system's built-in security protections.

This opens a device to a wide range of malware and targeted attacks. It's therefore important that your UEM/DM solution includes a means of detecting jailbroken devices, and defeating jailbreak jammers - software used to camouflage a device's rooted status.

Further, jailbreak and root detection should not be reliant on location services to trigger a test, which drains battery life and impacts user privacy.

MOBILE APPLICATION SECURITY & MANAGEMENT

Security through Containerization

Containerized apps provide IT with fine control by segregating each app and its data in its own dedicated, encrypted file store. Each app container can have its own usage rules or policies, and can be protected and wiped independently.

Personal apps installed by the device owner can reside safely alongside corporate-approved, third-party ISV apps or custom-built apps that interact with the intellectual property of the enterprise.

Because personal apps are isolated from corporate apps, they can be restricted from accessing the data in the corporate app containers (using native services such as copy and paste, for example). Yet users can still arrange both corporate and personal apps side-by-side or in any springboard configuration they desire.

If your UEM/DM solution provider offers appropriate Software Development Kits (SDKs), you can integrate security libraries directly into app source code before compilation.

While this method of containerization requires source code access and developers to do the coding, SDKs can potentially provide productivity benefits to developers and to the enterprise.

They can also enable developers to integrate new app features beyond just security capabilities, such as High Availability and Disaster Recovery services or even turnkey features to add to apps, such as user presence or printing.

At minimum, any containerizing solution should provide:

App authorization: (i.e., only allow the provisioning of an app to an authorized user's device).

App-level encryption: Using app-level encryption, independent from device-level encryption, means that even if a device passcode is compromised, the app data is still protected.

App authentication: Enable app-level password authentication with advanced options as needed, such as support for two-factor authentication.

Single sign on: Allow users to log in to one containerized app and gain access to all containerized apps, for a faster, smoother user experience.

Broad security policies: For example: strong passwords, data-loss prevention ("open in", cut/copy/ paste, file content management), and compliance controls (remote lock/wipe, detect jailbroken/ rooted devices, enforce OS version).

Secure access: To behind-the-firewall servers and other resources, that didn't require open inbound firewall ports or unnecessary exposure of the corporate network.

Digital Rights Management (DRM): File-level security policies to protect corporate content as it moves across devices, systems and clouds.

Deploying & Managing Apps

With the right solution for mobile application management (MAM), IT can provide employees and business partners the application and data access their roles require, on their preferred and personally owned devices, without having to take restrictive control of those devices to meet security and regulatory requirements.

Importantly, MAM policies and technologies can limit data deletion to selective wiping of specific enterprise apps and their data, leaving the rest of the device's personal content intact.

This way, mobility can be used as a true business enabler without compromising the user's whole device experience for the sake of corporate data security.

A corporate-brandable, private enterprise app store can provide a one-stop shop for distributing custom built or curated apps to employees and authorized members of the extended enterprise (e.g., contractors, ecosystem partners, etc.) - even when your IT admins don't manage the endpoint.

This way, IT can provide users with a consumer-like experience that's consistent across platforms, but with enterprise controls.

> Some solutions also include graphical dashboards to provide a detailed view of app adoption across the enterprise

This allows IT managers to zoom in on metrics such as registered enterprise app store users, number of apps in play, app istribution across OS platform, most popular apps and more.

CONSIDER THE FULL MOBILE APP LIFECYCLE

Your EMM solution should provide a framework for security and manageability for the entire app lifecycle, reflecting:

- App development and procurement (both third-party and
- in-house developed apps)
- App provisioning and deployment
- App security and policy management
- App usage and user feedback
- App decommissioning and selective data wipe

The following features are signs that IT Managers are moving in the right direction:

- Single-sign-on functionality, allowing users to only authenticate once in order to gain access to content across apps
- Encryption of data shared between apps, and in use by apps, no matter whether on-device, behind the firewall or in the cloud
- Easy containerization of any application
- An SDK that allows developers to take advantage of advanced functionality such as app-to-app secure document sharing, or a
- shared services framework for easily adding common features without writing new code

SECURITY CERTIFICATIONS & CREDENTIALS

What sort of security certifications do your shortlisted UEM platforms have? What about the vendors?

Depending on your industry, you may be required by law to seek a platform that can support your HIPAA, HITECH, GLBA, FISMA or other security requirements.

IT Managers should also pay attention to which organisations, analysts, customers and industries speak favorably of each platform.

Most vendors claim to have great security and boast about a checklist of features — but only the organisations with third-party validation can actually back up those claims.

Have they made the investment in time and resources to prove security is truly robust enough for your needs?

Mobile apps provide an open avenue for data leakage when employees send business data to personal cloud storage tools, personal email accounts and even perform device backups to personal computers.

But mobile security involves more than just the protection of business data in transit or at rest on devices.

Organisations also need to make sure they are securing the configuration details and user credentials that may be stored on mobile devices.

> Unprotected, they can create entry points that put your network and core business applications at risk

Securing the device alone doesn't prevent business data loss. IT teams must safeguard the three Cs of mobile security: content, credentials and configuration.

USER-PRIVACY PROTECTION

With the rise of BYOD, business and not for profit organisations have become increasingly aware of sensitivities and potential liabilities in how they manage employees' personal devices and information. Employees want privacy for the same reasons organisations want security.

What's theirs is theirs, and it needs to stay that way. Further, anti-discrimination laws in some countries can make accessing a device app inventory or geolocation information potential grounds for a wrongful termination lawsuit.

One of the most important examples of privacy infringement IT teams might face is when they fully wipe an employee's personally owned device because business data is at risk (e.g., due to a lost/stolen device or employee departure).

IT teams also need to be aware that requiring location services to enforce compliance (which can also drain batteries), or storing phone/location logs are potential infringements on employee privacy.

At Wanstor we suggest IT Managers look for a solution that will help build trust by protecting not only sensitive business data, but also workers' personal content, across operating systems, no matter who owns the device.

DOCUMENT CONTROL

File sharing — especially via mobile devices — has become an essential part of enterprise collaboration.

As business and not for profit organisations mobilize business processes, more and more sensitive data pass through and reside on mobile devices.

Files containing sensitive material such as intellectual property, financial data, and regulated information are therefore inherently at risk if left unsecured.

This is true regardless of whether they're shared within the walls the chosen organisation or with a third-party contractor.

It is a well known fact that once employees have access to a mobile solution they will be sending unencrypted emails, failing to delete confidential documents, or accidentally forwarding sensitive data to unauthorized recipients.

In order to prevent regulated or business-critical data from falling into the wrong hands, IT teams need to protect documents directly.

Seek a UEM/DM platform that offers a secure enterprise file synchronization and sharing (EFSS) solution with DRM (Digital Rights Management) capabilities to add file-level security policies, or one which integrates readily with such a tool.

In regulated industries, the IT department will need document tracking for auditing and compliance purposes, as well.

DEPLOYMENT MODEL (CLOUD OR ON PREMISES)

Many endpoint management solutions are available in both cloud (also known as Software as a Service, or SaaS) and on-premises versions.

There are advantages to each model. Among the factors that may play into your decision:

Deployment time: Cloud-based solutions can often be up and running very quickly.

Maintenance: Cloud-based solutions can lighten the load on IT when it comes to updates and upgrades, which is especially helpful for business or not for profit organisations with limited technical resources in house.

Access and control: An on-premises solution sits server-side in your datacenter. For some IT organisations, this provides a greater amount of control over data and disaster recovery, and tighter integration with other systems.

Compliance: For some high-security or regulated organisations (branches of government or the military, for example), regulations may make implementing an on-premises solution an easier choice - although as cloud deployments (and IT perceptions about them) evolve, this too is changing.

Ideally, a UEM/DM solution will make both deployment options available to the IT team, with no need to compromise on security or features however you choose to go forward, even if you need different models in different locations.

MIGRATION AND IMPLEMENTATION

Migrating to any new platform requires a commitment of time and resources. But the process doesn't have to be stressful. Choosing the right approach is critical — IT Managers want to be up and running with as few interruptions to employees as possible.

A UEM/DM strategy needs to account for this process. What resources does the IT Manager need and where will these come from? Typical enterprise customers have thousands of endpoints operating on different continents, from multiple offices around the world.

IT Managers need to have a transition plan for the migration phase, a schedule for these migrations and a training plan for both IT and end users.

TECHNICAL SUPPORT

You rely on your mobile platform — to speed up decision making, boost revenue and profit, facilitate workflow, and keep users, teams, customers and suppliers connected. It's business critical.

So when you're choosing your UEM solution, ensuring that the vendor offers the support capabilities and options you need makes smart business sense.

Find out exactly what's available, at what cost, to support your needs in planning, implementation, optimization and ongoing issue resolution. Otherwise, you're jeopardizing the gains that your UEM investment is meant to achieve in the first place.

TRAINING & USER FEATURES

What training support will you need, how will you access it, and at what cost?

The easier your UEM solution is for IT and for end users to interact with (both for initial provisioning and ongoing management), the less time you'll need for training — so be sure to find out what each potential vendor has done to streamline and simplify processes for these two key stakeholder groups.

PRICING & TOTAL COST OF OWNERSHIP (TCO)

Migrating to a single, unified endpoint management platform will help your organization standardize infrastructure, reduce complexity and increase ROI.

Be sure your solution can offer cost-effective and flexible mobility that can scale up or down as your needs change over time.

Insist on specifics when it comes to the number of devices you can add per domain.

Consider payment terms, too; if the idea of eliminating a heavy upfront capital expenditure is appealing, you may prefer a subscription model for more predictable yearly operating expenses.

Spreading out costs in this way can be helpful for cash flow. Lastly, to get to a full picture of TCO, you need to consider direct and indirect costs.

As you continue to move along the mobile maturity curve, reliability becomes increasingly mission critical.

ManageEngine Desktop Central Overview

To help business and not for profit organisations manage their IT estates, Wanstor has partnered with ManageEngine to design, deploy and manage their Desktop Central solution for customers in the UK.

Integrated Desktop & Mobile Device Management Software

Desktop Central is a unified endpoint management solution that helps IT teams manage servers, laptops, desktops, smartphones, and tablets from a central location.

By using a Desktop Central solution from ManageEngine, IT teams can automate regular desktop management routines like installing patches, distributing software, imaging and deploying OS, managing IT Assets, managing software licenses, monitoring software usage statistics, managing USB device usage, taking control of remote desktops, and more.

It supports managing Windows, Mac and Linux operating systems. It also helps IT teams to manage mobile devices to deploy profiles and policies, configure devices for Wi-Fi, VPN, email accounts and so on., apply restrictions on using cameras, browsers and so on, and to secure devices by enabling passcode, remote lock or wipe. IT teams can manage all iOS, Android and Windows smartphones and tablets using one tool.

The need for unified endpoint management

IT asset footprints are growing rapidly in today's business and not for profit organisations. Managing these assets has become more challenging for IT teams with the ever-increasing numbers of laptops, desktops, tablets, and mobile phones, which are otherwise known as endpoints.

The best way for IT teams to make sure devices are being managed properly is by employing endpoint management software. Endpoint management becomes even harder with varied devices, or with devices that travel outside of the organisation's network.

Benefits of unified endpoint management

Single-solution architecture	A single, centralised platform for endpoint management will help IT teams avoid complicated integrations among different software on multiple platforms. They will no longer need to compile, compare, and evaluate reports from different sources.
Ease of onboarding	A unified endpoint management platform allows organisations to easily push out device policies, applications, and environments, meaning devices go from out-of-the-box to in-use faster and with better baselining.
Helps improve IT security	Security is one of the primary concerns for any organisation today. Recent ransomware attacks just prove how dangerous zero-day vulnerabilities can be. A unified endpoint management solution makes it easy for IT admins to keep track of suspicious activities across all endpoints.
Improved visibility	Enterprises can monitor inventory, usage, vulnerable systems, and much more from one place. This visibility provides not only opportunities for cost saving, but also the ability to troubleshoot, diagnose, and resolve issues remotely.
Unified corporate IT environment	All the benefits of a unified endpoint management platform combine to deliver the single greatest advantage to organisations: a unified corporate environment in which experience is optimised across the organisation on corporate networks.

What is unified endpoint management?

Unified endpoint management is an umbrella approach to managing all the endpoint devices within an organisation from a central location.

In general, a typical unified endpoint management solution provides secure updates, patch management, automatic hardware and software inventory tracking, logging, mobile device management, software and OS deployment, workstation remote control options, license management, and overall quick remediation capabilities for IT professionals.

Key Desktop Central Features: Desktop Management

Desktop Management
Manage Windows, Mac and Linux

Windows 10

Patch Management
Automate patch deployment per OS and other third party applications, shield Windows and Mac from security threats

Asset Management
Manage your IT assets, Software Metering, Software License Management, Prohibited Software, and more

Active Directory Reports
100+ out-the-box reports provides a quick and complete insight of the Active Directory infrastructure

USB Device Management
Restrict and control the usage of USB Devices in the network both at the user-level and at the computer-level

Remote Control
Troubleshoot remote desktops with multi-user collaboration, file transfer, video recording, and more

Service Pack Installation
Scan and detect missing service packs of OS and Applications and automate deployment to stay up-to-date

Software Deployment
Simplify software distribution to install and uninstall software with built-in templates for package creation

Windows Configurations
25+ predefined configurations including Power Management, USB Device Management & Security Policies

User Administration
Define roles with selective privilege and delegate users to these roles for effective management

Power Management
Apply energy saving power schemes, shut down inactive computers and get system uptime reports

OS Deployment
Comprehensive disk imaging / deployment feature supports deployment needs in both offline and online mode

Mobile App
Start managing your desktops and servers on the go. Download mobile app for iOS devices

Key Desktop Central Features: Mobile Management

Mobile Device Management
Manage iOS, Android and Windows

iOS Windows 10

Device Enrollment
Enroll devices manually, in bulk or let users self-enroll their iOS or Android devices with two factor authentication

Asset Management
Scan to fetch details of installed apps, enforced restrictions, installed certificates and device hardware details

App Management
Distribute in-house and store apps to devices, remove or disable blacklisted apps, assign redemption codes for commercial apps and more

Security Management
Configure stringent security policies such as passcode, device lock to protect corporate data from outside threats.

Profile Management
Create, configure and associate policies and profiles for different departments, roles or groups

Audit and Reports
Audit mobile devices with out-of-the-box reports such as Rooted Devices, Devices with Blacklist Apps, etc.

In-depth focus: Asset Management

An IT administrator must be up-to-date on the information about the software and hardware used across the organisation they work for. Manual compilation and reconciliation of IT assets is effort-intensive and error-prone.

Desktop Central's web-based inventory management not only helps automate this task, but also provides out-of-the-box network inventory reports.

Inventory management features

- Perceive audit ready hardware and software inventory details.
- Schedule scanning of systems to collect inventory data.
- Manage software licenses, category, and compliance.
- Detect, block, and auto-uninstall prohibited software in the network.
- Have real time access to software usage statistics.
- Automate alerts on specific events such as installation or uninstallation of new software, removal of hardware, etc.
- Over 20+ out-of-the-box reports and the ability to create custom reports across different formats.

Scheduled inventory scanning

Desktop Central scans the Windows desktops and servers in the network periodically to collect hardware and software details and stores them in your the database. The inventory scanning interval is flexible and can be configured to meet the real-time needs of your organisation. This enables administrators to have access to up-to-date inventory information any time, without any manual intervention.

Alert notifications

Desktop Central sends email notifications to IT administrators for the following events:

- New hardware is added or removed in the network
- New software is installed or uninstalled in the network
- Non-compliance of software licensing policy
- Prohibited software is detected in the network

Hardware inventory

The hardware inventory provides complete details about the hardware used in the network. The hardware inventory reports helps IT administrators to:

- Sort computers by memory
- Sort computers by OS and service pack version
- Sort based on hardware manufacturers
- Sort by age, disk usage, type

Software inventory

Software inventory in Desktop Central gives IT Administrators access to:

- **Software metering:** Usage details of specific software such as number of times it has been used, total usage duration, systems with specific software etc.
- **Software details:** View commercial and non-commercial software information including vendor name, installation date, and software version.
- **Software license compliance:** Provides the ability to view the compliant and non-compliant software being used in the network.
- **Prohibited software:** Blacklist software, block executables through, and auto-uninstall prohibited software in the network.
- **Warranty management:** Track the warranty information of the hardware assets managed by your IT team.

Network inventory reports

Desktop Central provides out-of-the-box reports to view the software and hardware details of the network. These reports help IT administrators to gain a quick and accurate view of the network inventory.

The ability to export reports to PDF or CSV formats help integrate with third-party reporting engines or to print it out for future reference.

Achieving ROI from your Desktop Central Investment

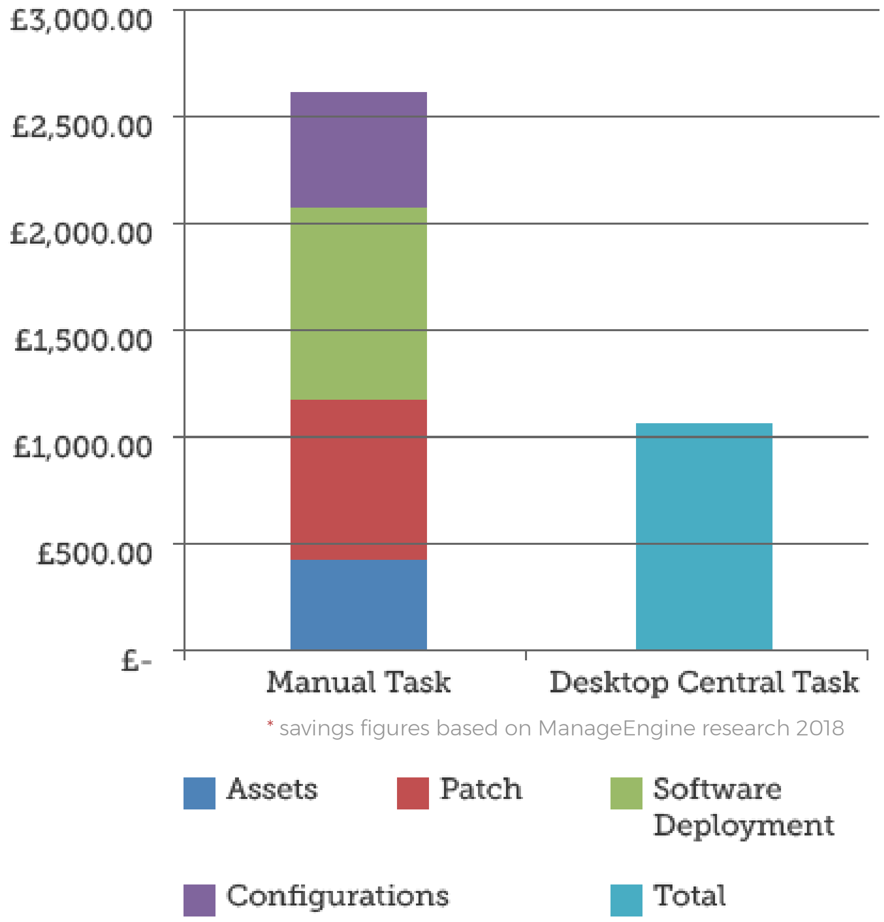
This example will demonstrate how Desktop Central saves IT teams, time, money and effort with a relevant and robust ROI calculation

Assumptions

- Network of 100 computers
- Hourly salary for a technician is £35

Notes

- While the cost of executing each task manually can be calculated, this is difficult within Desktop Central as it is integrated software. The graph to the right shows the total cost of performing these tasks using Desktop Central as opposed to manually.
- Whether IT teams do these tasks once or multiple times a year, the cost of doing it with Desktop Central is going to remain the same or may increase marginally, if you take into account the time spent by the technician in initiating the tasks from the management console



Manual task execution vs Desktop Central task execution

Task	Manual Execution		Desktop Central Execution		Annual Savings
	Man-Hours	Cost	Man-Hours	Cost*	
Performing asset scanning, patch management, software deployment, and configurations once in a year	114	£3,990	2.63	£1,087	**£2,903**
Perform Asset scanning once in a quarter, install patches once a month (excluding Microsoft Patches), install software and configure systems once a year	284.92	£9,972	2.63	£1,087	**£8,885**
Perform Asset scanning once in a quarter, install patches once a month (excluding Microsoft Patches), install software and configure systems once a year	484.84	£16,969	2.63	£1,087	**£15,882**

* includes an additional £995 towards the annual subscription fee for 100 computers

Comparing Manual task execution vs Desktop Central task execution

Procedure	Time per Computer	Time per 100 Computers (Manual)	Time per 100 Computers (Desktop Central)
Manual Scan to get hardware and software details	5 Mins	8.33 Hours	**2 Mins**
Identify missing patches for 3rd party applications like Adobe, Java, Firefox, etc.	3 Mins	5 Hours	**2 Mins**
Download required patches from the vendor's website and install them	5 Mins	8.33 Hours	**5 Mins**
Identifying missing Microsoft Patches	5 Mins	8.33 Hours	**2 Mins**
Downloading and Installing missing Microsoft Patches	5 Mins	8.33 Hours	**5 Mins**
Deploying simple software app	3 to 5 Mins	5 to 8.33 Hours	**2 Mins**
Deploying MS office applications	15 Mins	25 hours	**15 Mins**
Installing Service Packs	3 Mins	5 Hours	**2 Mins**
Configuring display settings, application settings, browser settings	3 Mins	5 Hours	**2 Mins**
Applying security policies, restricting USB device access, file restrictions	5 Mins	8.33 Hours	**5 Mins**
Local user management, mapping drives, installing printers	5 Mins	8.33 Hours	**5 Mins**

10 Reasons your IT team needs to purchase Desktop Central today

Integrated Desktop and Mobile Device Management Solution	▪ No need to rely on multiple tools for managing Desktops and Mobile Devices ▪ A single management console for all desktop and Mobile management tasks
Enhances Network Security	▪ Helps patch systems and applications automatically ▪ Enables administrators to apply windows security policies ▪ Restricts and customizes external device usages like USB, external hard disk, etc. in enhancing network security
Increases Productivity	▪ Robust support for BYOD ▪ Fosters collaboration between employees with their mobile devices ▪ Enables employees to access corporate resources from anywhere
Manages Distributed Environment	▪ Manages geographically distributed computers, devices and users from a central management console ▪ Allows setting up distribution points to minimize the WAN bandwidth consumption ▪ Provides control on mobile devices irrespective of location
Higher Return of Investment (ROI)	▪ Saves operational costs by automating various routine activities like Patch Management, Software Deployment, mobile application ▪ Manages BYOD and save costs from investing in new devices ▪ Enable and set up Power Management to see immediate savings on desktop power consumption ▪ Effective software license management will save cost of unused licenses ▪ Accessing asset information, installing software, tracking tickets now performed within single console i.e. by integrating Desktop Central with Service Desk Plus
Reduces Training Costs	▪ Simple point and click installation package includes an embedded relational database and webserver ▪ Saves working with multiple packages reducing training costs by providing a simple, user-friendly interface
Completely Web-based	▪ Completely web-based offering unparalleled flexibility in accessing the systems and mobile devices from anywhere
Integration with other ManageEngine Products	▪ Seamless integration of data with ManageEngine ServiceDesk Plus and AssetExplorer ▪ Help Desk and Desktop Management functions can be performed from single integrated console ▪ Integrates with ManageEngine Products such as Servicedesk Plus and IT 360 Applications
Easy Installation & Setup	▪ Single installation package including all required installables such as database and web-server ▪ Installation within 10 minutes and setup within one hour
Affordable Solution	▪ Offers competitive price and ease of deployment on standard hardware, supporting desktops, mobile devices and servers ▪ Accustoms without steep learning curve

Wanstor Customers using ManageEngine Desktop Central

Final Thoughts

Today's modern worker is no longer confined to a physical office or a Windows desktop or laptop. Although traditional Client Management Tools (CMT) would have been sufficient in the past, they are no longer enough to manage the increasing diversity of platforms and devices, BYOD, and frequent Windows 10 updates.

While many business and not for profit organisations have adopted Enterprise Mobility Management (EMM) solutions to manage mobile endpoints, maintaining both CMT and EMM without any integration is highly inefficient. Instead, IT teams need to select the right Unified Endpoint Management (UEM) solution.

Unified Endpoint Management combines traditional Client Management with Enterprise Mobility Management providing the IT team with a single view to manage devices, apps and data.

For more information about Wanstor and ManageEngine's Desktop Central solution please email us at **info@wanstor.com** call us on **0333 123 0360** or visit us **here.**