IT Asset Management: Insights into best practice

A Wanstor Quick Guide

wanstor

Contents

wanstor

Introduction

At Wanstor we understand that IT has become more end user focused than ever before.

IT teams are now led by the user experience and not the other way round where IT used to dictate terms on what users could/couldn't have access to in terms of IT assets.

This change in how IT is viewed, used and perceived within organisations has meant IT hardware, software and overall infrastructure estates have grown exponentially over the past 5+ years.

Each day new users are being added to the corporate network and with new users comes new devices and IT assets – hardware and software. It is usually the responsibility of system administrators to track and manage IT assets.

However as the amount of IT assets has grown substantially over the past 5+ years, many system administrators are now at an IT Asset Management tipping point.

They only have so many hours in the day and are being asked to be responsible for more and more devices across a more diverse end user base than before.

At Wanstor, we believe there has to be a better way for system administrators to manage ever growing and more complex IT estates.

Wanstor's IT experts believe that many potential IT issues could be resolved quickly, efficiently, and with better IT administration support, if system administrators have access to the right visibility tools into all the IT assets that exist in their IT landscape – network, data centre, remote sites, user workstations, etc.

What is IT Asset Management?

First of all it is important to define what we mean by IT Asset Management. At Wanstor we believe IT asset management (ITAM) is a set of business practices that join financial, contractual, and inventory functions to support life cycle management and strategic decision making for the IT environment.

Managing IT assets allows IT Managers to get maximum value from the use of the assets they have purchased and are responsible for, right-size IT inventory, and optimise inventory purchasing decisions and strategies. IT asset management provides IT Managers and system administrators with the means to achieve complete visibility into their IT infrastructure inventory, helping them to gain an in-depth understanding of:

- What systems and equipment exist
- Where components exist and are housed
- How they are used and who they are used by
- What they cost (OPEX vs CAPEX)
- When they were added to the inventory
- Whether they have an expiry date
- How they impact IT and business services

By having this level of visibility into IT asset details, IT teams can improve infrastructure efficiency and performance, and minimise related overhead expenses.

All business and not for profit organisations, in some shape or form, perform ITAM. However just saying and following a basic ITAM programme is no longer *"good enough"*.

Only doing the basics will get IT teams so far. However in an ever changing, growing and complex IT environment it's important to implement ITAM practices intelligently.

By choosing the right processes, tools and people for ITAM, only then will IT teams be able to achieve IT operational efficiency, financial accountability of asset purchase, simpler auditing and compliance, and long-term asset manageability and maintenance.

In this document Wanstor's IT Asset Management experts have focused on the benefits of proper IT asset management, best practices, and how to implement it, so it benefits your IT teams, business, end-users and employees.

IT Asset Management: Suggested methodology

The major goal of ITAM is to establish a centralised asset repository that accounts for the presence and purchase of all hardware and software inventory. To achieve this, Wanstor believes ITAM methodology is made up of the following steps:

- **Asset discovery, data capture and storage:** Discovering all hardware and software components of IT inventory on the IT infrastructure and capturing their details, such as the type of asset, make, specification, etc., and storing it in an asset repository
- **Asset tracking:** Being able to identify and track change in the location of assets, increase or decrease the number of assets, track assignment status and user information
- **Asset lifecycle management:** Being able to capture the asset lifecycle data right from requisitioning, purchase and assignment, to expiry and decommissioning
- **Asset reporting and alerting:** Being able to generate asset inventory reporting, and receive alerts on asset warranty and lease expiration

wanstor

By implementing a centralised ITAM process and asset repository programme IT teams will be able to support various ITIL functions, such as configuration management, incident management, problem management, and service level management.

Whilst looking to build a centralised asset repository, it's important to understand the difference between asset repository and configuration management database (CMDB).

The CMDB is a development of the asset repository which is part of the ITIL framework. Beyond the scope of asset discovery and tracking, the CMDB is integrated with service desk functions and is part of IT service management and change management.

Hardware Asset Management

Hardware asset management is the process of tracking and managing the physical components of computers and computer networks, from acquisition through to disposal.

The objectives of hardware asset management are to be accountable and responsible for all hardware assets on the IT infrastructure to provide comprehensive inventory visibility.

Additionally hardware asset management should provide details, to help IT teams with vendor contract and lease management, and to assist in making budgetary forecasts based on the stock of assets and business requirements now and in the future.

Software Asset Management

Software asset management is similar to hardware asset management, but is purely focused on software assets, including licenses, versions, and installed endpoints.

ITIL states that the goals of software asset management are to reduce IT costs and limit business, legal and security risks related to the ownership and use of computer software, while maximizing IT responsiveness and end-user productivity.

In the next section we will investigate the various benefits of IT asset management and some best practices IT Managers can take into their existing IT frameworks.

Asset Lifecycle Management

Whether it is hardware or software, there should be a disposal or replacement date.

Asset management allows IT teams to keep track of when a hardware is purchased, how long has it been used, whether there's a lease expiring on the component, etc.

For system administrators, it is important to know what version of software and how long your end-users have been running this software on their system, and whether their OS is current.

This is actionable data IT teams should use to decide if they should replace old or faulty hardware, uninstall or patch a vulnerable application, or update the firmware on the system.

The IT Manager should also familiarise themselves with vendor contracts and relevant asset information.

This will give them the knowledge as to when to extend or renew a contract with vendors or hardware/software provider based on contract, purchase order, and expiry information fed into the asset management system.

Strategic Inventory Planning & Procurement Forecast

When IT Managers keep track of what inventory they have in their IT infrastructure, it becomes easier to plan for future spending on assets. Without knowing what currently exists in end-user systems – both hardware and software – it is very difficult to plan a procurement budget.

In many cases Wanstor has actually seen IT Managers over purchase IT assets as they do not know what they actually have and why they need new assets when they may already have some in stock.

Centralised and streamlined asset management enables IT Managers to scan their entire network and list which hardware and software systems are using. Being able to collectively view inventory data with storage capacity of end-user systems is useful for storage utilization analysis and budget planning.

This information becomes critical as IT Managers start financial planning, allowing them to plan well in advance for future asset needs, and maximizing existing asset utilization and eliminate unnecessary expenditure.

Increased Accountability to make sure of Compliance

Keeping track of IT inventory and automatically updating it using asset management systems will help IT Managers to monitor hardware and software components of their network computers, and identify whether unapproved or harmful software or hardware is installed.

Making sure compliance with corporate security policies and desktop standards is a must for all business and not for profit organisations.

> ## Efficient asset management of IT inventory will help IT Managers to achieve their financial goals

By allowing system administrators to quickly isolate vulnerabilities, such as illegal/unauthorized software, outdated software, games and unauthorized/malicious downloads, an ITAM system makes it easier to see where potential risks may exist, so they can be prevented before major problems arise.

This helps IT Managers to keep systems and assets compliant, and provide IT inventory reports for compliance auditing.

Automated Asset Discovery & Tracking

Many business and not for profit organisations manage their IT asset inventory using manual, paper-intensive processes, which drain resources and are highly prone to inaccuracies and inconsistencies. Spreadsheets are used by many IT teams to manually enter details of the assets and then they constantly have to modify assets as they update.

With the introduction of IT asset management solutions and asset management integrations with systems and network monitoring tools, this process can be made simpler, quicker and easier to manage.

ITAM systems like desktop central by ManageEngine for example perform automated device discovery on your enterprise LAN. For example, if there are Windows servers and operating systems on your network, then using WMI, the ITAM tool can discover the Windows nodes and fetch all hardware and software asset information from them.

With the pace that enterprise networks are growing and IT systems are getting updated, an automated asset management method is in Wanstor's opinion "a must have" to constantly keep abreast of asset updates and changes. Automated ITAM considerably saves manual effort and time, and results in a lower number of errors and staff overheads.

What is the core benefit of ITAM?

Gain Control Over IT Inventory

If IT departments are undertaking an effective asset management practice for their business or not-for-profit organisation, they already realise benefits from deeper visibility into hardware and software assets. This means IT Managers and support personnel should investigate further into viewing and managing asset details of the end-user system.

Asset management allows easy viewing of hardware and software components of a computer, server, or of any other network infrastructure. Traceability of assets across their IT landscape gives IT teams better IT administration control and accountability.

Using an automated asset discovery and management functionality, along with a server and application monitoring tool will allow IT Managers to see the computer inventory details, all whilst actually troubleshooting a server crash or application performance issue. IT Managers can also discover if an employee has any unauthorised and non-compliant hardware or software on their enterprise workstation.

A server or workstation will benefit from asset management data covering:

- Drivers
- Firmware
- Graphics and Audio
- Hard Drives
- Hosted Virtual Machines
- Logical Volumes #
- Memory
- Network Interfaces
- Operating System Updates Applied
- Out of band management
- Peripherals
- Ports and USB Controllers
- Processors
- Removable Media
- Software Inventory
- Storage Controllers
- System Information
- OS Update Information

Best Practices for Implementing IT Asset Management

Asset Management via Server & Application Management systems

For IT admins, application performance management (APM) is crucial to making sure undisrupted business service through high availability and performance of applications and server infrastructure.

Incorporating asset management as part of an APM solution will help IT Managers identify the right server assets, what's installed in the server, whether the server has an expiring lease and warranty, or storage capacity, while they actually troubleshoot and remediate application or server hardware health issues.

Asset Management via the IT Help Desk

At Wanstor we believe it is sensible to incorporate asset management into your IT help desk function. IT is ultimately the hardware and software assets that users are creating trouble tickets and service requests for.

Being able to capture the entire asset data of IT inventory including purchase order, parts and billing information will be useful for the IT help desk support team.

It will be even more beneficial if the help desk is able to associate and tag trouble tickets with specific assets so they can track the history of service requests.

Integrating asset management with help desk results and a more efficient ITIL support, change management and overall service request fulfilment.

Asset Management with Patch Management & Software Distribution

A patch management solution scans systems for critical and vulnerable software and third-party applications that need to be updated to mitigate security risks.

Once the systems with vulnerable applications, and the applications themselves are identified, then the system administrator will patch them with the latest version of the software or operating system.

Asset management plays a crucial role here as all the servers, workstations and notebook assets on the IT environment have to be discovered first and then their software inventoried.

Asset Management with Network Configuration & Change Management (NCCM)

The application of asset management is a little different with NCCM as it applies more to network devices, such as routers, switches and firewalls.

As network administrators use network configuration & change management tools to manage device configurations, it's also important to the management of network device inventory.

NCCM solutions offer a device end-of-life (EOL) management feature that helps IT Teams manage the lifecycle of network assets, who the manufacturer is, and when the product will be EOL'd.

This will help in preparing budget forecasts for product maintenance renewal and device replacement planning.

wanstor

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.

wanstor

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.

wanstor

Key Desktop Central Features: Desktop Management

Desktop Management
Manage Windows, Mac and Linux

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

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

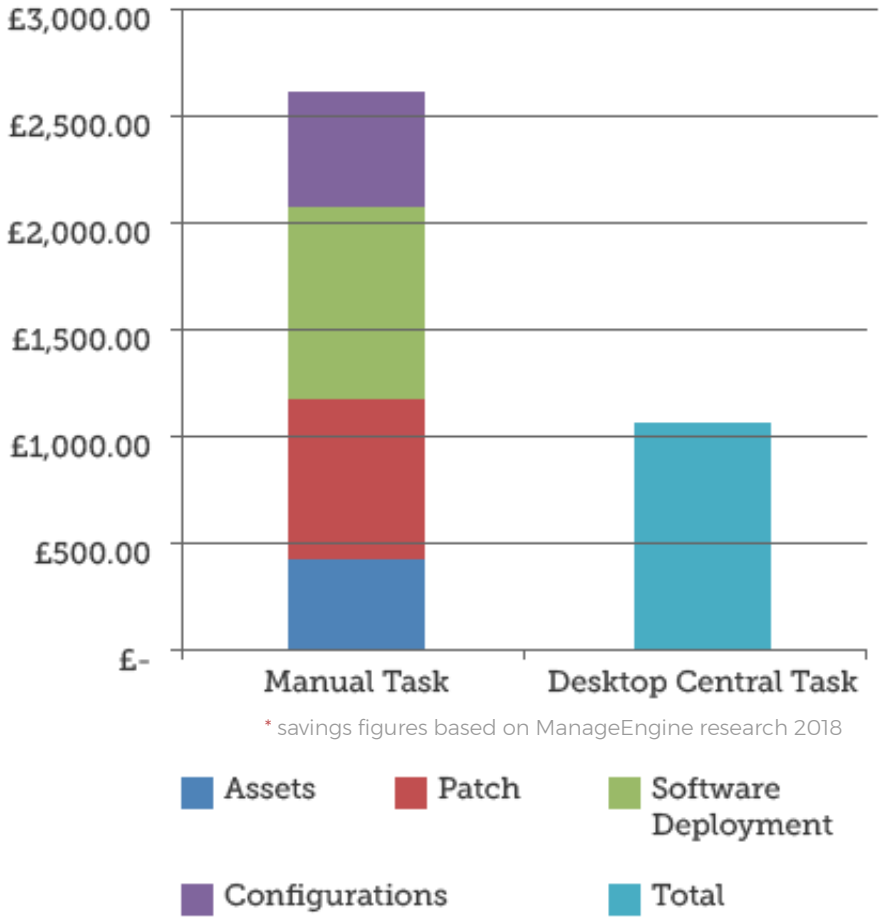
This example will demonstrate how Desktop Central saves IT teams, time, money and effort with a relevant and robust ROI calculation

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



* savings figures based on ManageEngine research 2018

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**.

Wanstor | 124-126 Borough High Street | London | SE1 1LB |

info@wanstor.com