Successful IT Asset Management:
Selecting the right processes and tools

White Paper

wanstor

Contents

wanstor

IT Asset Management: Why it's important

An effective IT asset management (ITAM) programme can deliver significant benefits through IT cost management, increased agility and reduced risk. Gartner regularly report that clients who successfully execute ITAM as a discipline typically achieved 30% cost savings in the first year, and at least 5% cost savings in each of the subsequent five years that they have a programme in place.

In addition to monetary savings ITAM can also significantly reduce the compliance risks associated with the recent increase in software audits and security scares and free up IT people to concentrate on more strategically important tasks.

At Wanstor we define IT Asset Management as a framework and set of processes for strategically tracking and managing the financial, physical, licensing and contractual aspects of IT assets through their life cycle.

ITAM experts at Wanstor believe there are three elements that are essential to realise the value of IT asset management:

- A focus on financial, contractual and physical data
- The asset life cycle
- A process framework

Few business or not for profit organisations today could function without the IT assets – the hardware, software, network and other technologies – that support their daily operations.

Not only are IT assets constantly evolving in terms of numbers per user, they are expensive to acquire, configure and maintain. Additionally IT assets are frequently moved, rapidly depreciate and require constant updates and replacement.

The overarching objective of IT asset management is to make sure the large volume of constantly churning, costly assets so essential to a business or not for profit organisations success are effectively managed from beginning to end to achieve the highest possible return on investment.

ITAM focuses on the centralized management of financial (e.g., purchase price, cost events, supplier, etc.), contractual (e.g., terms and conditions, software entitlement, support agreements, leases, warranties, etc.) and physical (e.g., location, ownership, assignment, etc.) data about IT assets in a business or not for profit organisation.

It is a completely different function than IT operational management, where the main objective is to optimize the performance and delivery of IT services.

wanstor

Additionally configuration management is not IT asset management.

Configuration information derived from IT operational management tools should never be used as a substitute for IT asset management data sources like ERP (enterprise resource planning) and finance systems.

For example, asset assignment should not be based on the discovered primary user of a computer, nor should an asset's physical location assignment be determined by IP address.

Using configuration information in place of properly sourced data is not consistent with IT asset management best practice

Although it should be noted that ITAM and configuration management are closely linked to overall IT operations success.

wanstor

IT Asset Life Cycle

Life cycle management practices are required and known to improve the return on investment for IT assets, avoid internal and external audit consequences, and adopt future technology. At Wanstor, we believe in five stages to an asset life cycle: requisition, procurement, deployment, maintenance & retirement.

Whilst many IT teams mistakenly believe that IT life cycle management begins when they receive an asset, the life cycle actually starts when an asset is requested. Correspondingly, life cycle management continues after an asset is no longer operationally active, extending to retirement and disposal activities.

Management of the life cycle is likely to continue for an indefinite period where historical asset records must be retained to satisfy legal and fiscal requirements. Effective IT asset management requires complete coverage of the entire life cycle.

As an asset progresses through the life cycle, its status changes, and changes will occur to financial, contractual and physical data associated with the asset. Simply recording and tracking these changes, however, does not constitute asset life cycle management. Asset tracking IS NOT life cycle management!

Figure 01

IT Asset Life Cycle

Requisition Procurement Deployment Maintenance Retirement

Source: Gartner, May 2013

wanstor

IT Asset Management: Process and best practice

Following the IT Asset Management Process Life cycle is what IT teams do, and asset tracking records is what they have done. The process is how you do it. Process is at the heart of IT asset management. It's all about process.

Peter Lukes, Managing Director, Wanstor knows how important the process and tool support in managing assets through the entire life cycle actually is and comments: *"ITAM depends on robust processes, with tools to automate manual processes. This data enables business or not for profit organisations to effectively manage IT assets, vendors and a software and hardware asset portfolio from requisition through to retirement. This means IT teams can monitor the asset's performance throughout its life cycle."*

A process is a sequence of activities and tasks for the management of assets through a particular step in the life cycle. Effective processes are designed to achieve specific goals and objectives, take into account corporate policies, standards and procedures, and are modelled on established and proven industry best practices.

Proper processes provide control, consistency and accuracy. Well defined processes that are structured, enforced and automated in a supporting tool are the foundation for IT asset management success.

Best Practice

The quality of processes implemented in support of an IT asset management programme is critical, especially for automated processes that are not under direct human supervision.

At Wanstor we believe best practice is capturing proven and effective know-how and incorporating it into IT asset management processes.

Apart from the specialized ISO 19770 standards and Microsoft® SAM Optimization Model for software management, no generally recognized framework is available for IT asset management.

Best practice makes sure process is optimised based on successful individual and aggregated experience and is directly integrated into better IT asset management tools.

wanstor

There are, however, three good sources for best practices:

- **Effective current practices:** Whether or not there is an existing IT asset management programme, practices already exist to perform IT asset management functions. In many cases, these practices have been refined over many years to become more effective and better matched to an organisations requirements. At Wanstor, we believe there is no substitute for practical learning. Taking the time to identify, formally record and embed successful methods into an IT team's culture is the most fundamental and important source of best practices.

- **Industry:** Organisations like the International Association of IT Asset Managers (IAITAM), publications like the ITAM Review, and ITAM events and webinars are excellent sources of best practice information. Experienced IT asset management and software asset management consultants can also provide valuable knowledge and insight.

- **Tools:** Superior IT asset management tools integrate best practices directly to make sure tasks and activities are performed in the correct sequence, that appropriate relationships and interdependencies are taken into account, and that data is properly maintained and updated. For example, a good ITAM tool will move child assets when the parent asset location is changed, or remove software assignments automatically when a hardware asset is retired.

wanstor

How mature is your IT Asset Management?

There are a number of different maturity models that establish an IT teams level of proficiency and guide future improvement. These include Gartner's ITScore for Infrastructure and Operations (ITSIO), and the Microsoft Core Infrastructure Optimization (CIO) model.

Regardless of the model, it is universally agreed that:

- Most medium sized business and not for profit organisations are at a low to modest level of IT asset management maturity.

  In its five-level model, Gartner estimates that about 35% of enterprises have reached the proactive (3rd) level of ITAM process maturity, while 5% to 8% have reached the service-aligned (4th) level, and less than 3% have reached the business partner (5th) level.

- Increasing benefits accumulate as maturity level increases. As IT teams progress from level to level up the maturity curve, each step will yield incremental savings, resulting in lower costs, decreased risk and increased business alignment.

- Maturity increases as a result of process improvement and implementation of tools that provide effective process support and automation. For example, these are characteristics of IT teams at the proactive (3rd) level of the Gartner ITAM maturity model: At this level, asset management teams should have designed, documented and tested the processes that are being adhered to around the different stages of the life cycle.

Another characteristic of this level is that an ITAM repository and at least one inventory tool and software usage tool should be installed and delivering day-to-day reports regarding the performance of the assets.

These tools will help automate processes, thereby reducing the need for manual data entry, such as contract data or hardware inventory data collection, which will lead to a higher degree of data accuracy.

Continuous process improvement combined with effective tools that provide process support and automation advance IT asset management maturity to deliver increasingly greater benefits.

wanstor

Building a successful ITAM programme

In order to realise the significant potential benefits of IT asset management, a successful ITAM programme requires breadth and depth.

Specifically, breadth of life cycle coverage and depth of process support. Making continuous improvements to processes results in increasingly greater benefits.

By integrating IT life cycle management processes through all the stages of the asset life cycle, IT asset management (ITAM) programmes can contribute meaningful savings at each stage.

Successful IT asset management programmes are supported by effective tools.

An effective tool is characterized by its ability to manage financial, contractual and physical data, integrate with adjacent IT management tools and business systems, provide out of the box best practice functionality, and support implementation and automation of IT asset management processes.

At Wanstor, we firmly believe that those who systematically manage IT asset life cycles focusing on processes augmented by tools will reduce costs and improve the performance of the IT assets in their environment.

What makes a successful IT asset management programme?

- Complete coverage of the entire IT asset life cycle, from requisition to retirement (or beyond)

- Well defined processes to make sure efficient, consistent and accurate execution of IT asset management tasks and activities

- Continuous process improvement to achieve increasingly greater levels of maturity

- Effective tools that provide process support and automation.

wanstor

Selecting the right tools to support

Wanstor's ITAM experts believe there are four core capabilities tools must provide to support an effective IT asset management programme:

- An IT asset management repository

- Hardware and software inventory and usage information

- Integration with adjacent IT and business systems

- Data importation

The IT asset management repository is the main component of an IT asset management system. It serves as the central store for the required financial, contractual and physical data.

However, what determines the quality and effectiveness of the tool is the repository's functional ability to perform IT asset management tasks and activities that support processes across the life cycle and that are based on best practice.

The ability to discover hardware and software inventory and determine asset use is essential to effective IT asset management.

wanstor

Both automated discovery and physical inventory tools like bar code scanning are required to make sure continuous management of assets through both operational and non-operational portions of the life cycle.

Without physical inventory capabilities, it is impossible to support certain IT asset management processes and best practices, such as receiving and rolling (physical) inventory.

Additionally IT asset management is reliant upon data from both IT and business systems.

Wanstor recommends that when choosing an ITAM repository, (based on feedback from over 100 of our customers who have selected ITAM tools with us) they say one of the top priorities is to identify and review how tightly integrated the repository is with adjacent toolsets.

Other toolsets with which ITAM repositories will integrate, besides inventory and software usage, are IT service support management, change management, and purchasing and configuration management.

As a minimum, an import tool should be able to access information stored in either databases or files. This tool should provide capabilities to filter and transform source data to either create or update asset records in the repository.

Where no direct technical integration is provided, effective data import capability is required, e.g. from finance or ERP systems

Given the increased benefits that are realised as an IT asset management programme evolves, it is essential to select a tool whose feature set will meet current needs, and support anticipated future requirements as maturity improves.

A larger initial investment in a more highly functional tool at the outset can prevent significantly higher downstream costs associated with tools who's functionality fails to keep pace with organisational improvement.

wanstor

Evaluating IT Asset Management Tools and Vendors

It's essential to thoroughly assess and evaluate relevant ITAM tools. At Wanstor, we recommend the preferred method of evaluation is through direct use of fully functional trial or evaluation versions.

This provides an opportunity to rigorously test software with real data and fully explore integration with existing systems and environments.

Along with a functional assessment, a detailed review of product documentation will help establish the tool's capabilities and quality. In light of or as a supplement to hands on testing are product reviews and evaluations by objective and knowledgeable third parties. For example, decision makers should take a look at Gartner' Forrester and IDC's recommendations of ITAM tools.

Product reviews are also occasionally featured in industry periodicals and web sites; however, caution should be exercised in using information acquired from general forums and blogs, even those hosted or moderated by a credible authority - particularly when information is posted by unattributed sources or anonymous authors.

Reputable tool vendors will be able to provide customer case studies and references. While partisan, these can be useful in more clearly understanding capabilities or scenarios that are particularly relevant or specific to a certain business need or industry.

In addition to evaluating the quality and appropriateness of the tool, due diligence is also required in appraising prospective suppliers. At Wanstor, we believe the most important assessment criteria include:

- Established experience in IT asset management and software development

- Future viability (past track record and length of time in operation)

- Evidence of success and expertise, such as industry memberships, awards, accreditations and certifications

- Company priority and focus on IT asset management software development (as opposed to professional services, development focus on other software products, etc.)

- Established history of product introduction and innovation in the ITAM marketplace

wanstor

Demonstrating value from ITAM

IT Managers responsible for IT asset management must demonstrate and quantify IT asset management programme benefits, to secure vital resources and ensure ITAM is a valued component of IT, developing outcome-oriented metrics to quantify value and ROI delivered through ITAM practices.

Key Challenges to IT Asset Management Success

- IT asset managers struggle to demonstrate and quantify value in order to justify continued executive sponsorship and investment in IT asset management tools

- Many ITAM teams are already suffering from a lack of skilled staff and are unable to prioritise programme value assessments. This means reporting this value could provide the justification for much-needed additional head count and tools

- Tracking ITAM benefits is a time consuming exercise, especially when trying to use a methodology that is accepted across the business or not for profit organisation. However if IT Managers are not prepared to put the time into proving the benefits of ITAM how are they supposed to secure the right levels of funding for it?

- IT Managers are often unsure what types of metrics to use to demonstrate ITAM value that is meaningful to the business

wanstor

Wanstor recommends that IT managers responsible for ITAM programmes should:

- Evaluate all ITAM life cycle processes (requisition, procurement, deployment, maintenance and retirement) to investigate them for delivered benefits

- Align ITAM metrics to critical business and IT initiatives, goals and objectives. They should make sure that values with the maximum impact are measured

- Analyse the logic behind ITAM benefits calculations to ensure their validity. For example - Consider using an internal audit to add credibility to ITAM value metric processes and methodology

- Maintain an ongoing log of all cost savings/avoidance that can be attributed to ITAM program efforts, such as the cancellation of unused / unneeded hardware maintenance, software licenses and/or maintenance or services contracts

As identified in the previous section of the document, IT Managers quite often struggle to demonstrate and quantify value in order to justify continued executive sponsorship and ongoing investment in ITAM resources.

These managers want to establish best in-class ITAM practices that demonstrate value, but they struggle to accomplish this with limited resources, such as head count.

ITAM budgets are often at risk of becoming stagnant or, in the worst case, shrinking. Unfortunately, without a clear business case to demonstrate the need for increased resources, ITAM teams can usually expect more of the same.

Business cases require hard facts, relevant ROI calculations and proven financial benefits to be approved

By having an established set of ongoing, monitored ITAM value metrics, IT Managers can help ease this process.

So how do ITAM teams demonstrate and promote their value? What should we really track and measure?

As already identified, many IT Managers believe it's too time consuming to track accomplishments when there are more pressing issues at hand. Even when there is adequate staff to perform the task, tracking benefits is often not a priority.

wanstor

The problem with this opinion is that if there is no perceived or validated value delivered to the enterprise, ITAM budgets will continue to be at risk of stagnation or reduction.

This usually results in insufficient funds for critical ITAM resources. In order to begin measuring and communicating ITAM program benefits, IT Managers should follow these steps:

- Determine what is important to your business and IT in terms of objectives and desired outcomes

- Mine existing ITAM processes for activities that link to these desired outcomes

- Define what outcomes can be effectively quantified and tracked

- Develop an ongoing discipline of tracking ITAM benefits that includes measurement validation and results communication

We believe the key to success is to map the priorities of your particular business to the value delivered through your ITAM discipline in the various areas of importance to your business and IT

As discussed throughout this document ITAM activities are important for several reasons. In recent years, due to many IT budgets shrinking there has been a heightened focus on ITAM activities and as a result of an increase in software license compliance audits.

However, there are many other reasons why organisations must aim to establish or improve ITAM practices.

A good starting point to demonstrate how ITAM can show value back to the business is the effective management of the high-risk end state of the IT asset life cycle – retirement and disposition.

Robust ITAM programs focus on the two major areas of IT asset disposition (ITAD) risk: data security and environmentally-responsible recycling.

All IT teams should make sure that their ITAD vendors have rigorous data sanitization processes and a robust recycling process.

IT Managers responsible for ITAM should communicate the importance of such robust ITAD processes and the substantial risk to their business or not for profit organisation from ineffective ITAD.

Quite often the benefits of ITAM may be difficult to quantify and project. However, they are very material in a financial sense, particularly from a brand equity perspective.

Just as IT Managers may be able to manage risks within a supplier agreement through improved terms and conditions, there is no specific financial number associated with this activity to measure its success; however, these instances should still be tracked.

Measurements of risk avoidance from proper asset disposal practices are worth tracking and communicating, especially if there have been fees or violations of ITAD's stringent regulations in the past.

Document regulatory compliance (including fines avoided) as part of your benefits-tracking discipline.

Top benefits for organisations implementing an ITAM programme

- ➕ Control of IT Assets
- ➕ Cost savings across hardware and software
- ➕ Financial Management of IT (Improved cost & benefit analysis)
- ➕ Better Financial Analysis of IT Sourcing Options
- ➕ Improved Operational Efficiencies across the IT department
- ➕ Licence Compliance
- ➕ Inventory Accuracy
- ➕ Improvement of Configuration Management
- ➕ Re-use of software
- ➕ IT security risk reduction
- ➕ Cost avoidance & avoidance of IT overspend

Another example is where organisations develop sustainability or 'green IT' programmes – it is probably worthwhile investigating ITAM metrics that show progress toward these goals. Many such programmes are focused on reducing carbon footprint and environmental waste. For organisations that have environmental objectives as a priority, it is worth measuring the value of moving to recyclable materials for all hardware items. Such organisations could also place a value on changing asset disposal methods from landfill-based disposal to vendors that make sure disposed items never end up in landfill.

Most business and not-for-profit organisations maintain highly sensitive information, where the risk of its exposure at endpoints such as PCs or mobile phones is a concern. Security risk metrics as part of an ITAM programme would therefore be beneficial to track.

Where potential losses can be tracked and recovery rates can be proven, incidents and successful mitigation can be reported - for example, the number of times the ITAM process was able to successfully wipe data from endpoint devices when they were reported lost or stolen. In some cases, a monetary value may be established, or at least estimated, for such avoidance of data loss.

IT Managers should align their ITAM value metrics with critical business initiatives to maximize the impact of results. In summary the more tightly integrated ITAM practices are with key business goals and objectives, the more indispensable ITAM will be to executive management.

Wanstor's key metrics for consideration when demonstrating value of ITAM disciplines

+ Number of unused / unnecessary maintenance or support contracts (hardware, software and telecom) terminated, their associated values including avoidance of any cancellation, escalation or late fees
+ Licenses and assets redeployed, refurbished or upgraded versus purchased (determine costs based on current vendor contracts or comparable substitute products)
+ Percentage of hardware leases refreshed on or before lease end date, as well as any buyout negotiations that provide value versus continuing with monthly payments
+ Number of purchase orders reduced determine via procurement team the cost of cutting one purchase order to a vendor
+ Successful audit results, which can be defined in a variety of ways
+ Success for your entity, based on its history, may be a compliance invoice of only 5% (or less) of the current contract value. Capture any costs avoided, such as fees you would have to pay to auditors if you are found to be non-compliant
+ Audits deterred / decreased by demonstrating solid ITAM / software asset management (SAM) disciplines that convinced a supplier to withdraw an audit request, or at least cease annual audits in favour of less frequent ones
+ Reduction in total number of titles, identical line items and / or number of suppliers in portfolio based on ITAM practices
+ Movement, transfer or divestment of IT assets through increased visibility and improved contract terms and conditions
+ Proactive elimination of license purchases and / or non-standard equipment through policy enforcement
+ Reduction in cycle times for planning and executing major software licenses, maintenance and support renewals

Sustainability Example : Drivers and Measures

Value	Drivers	Measures
▪ Pollution Cost, Impact and Risk Reduction	▪ Pollution and waste ▪ Resource consumption ▪ Changing energy and resource economics ▪ Environmental externalities ▪ Compliance costs ▪ Supplier engagement: material / product reporting and insight	▪ Pollution prevention ▪ Cost reduction and efficiency improvement ▪ Improved risk visibility and management ▪ Tangible connections between sustainable and finance outcomes ▪ Enriched supplier interactions, shared savings and collaboration
▪ Reputational Legitimacy	▪ Transparency ▪ Compliance ▪ Communications and corporate social responsibility (CSR) ▪ Green brand power and the green marketplace ▪ Supplier engagement: social responsibility and labour standards	▪ Product leadership and management ▪ Enhanced stakeholder relations ▪ Reputations and legitimacy ▪ Product portfolio re-evaluation ▪ Supplier risk reduction

Develop a Standard of Benefits Measurement and Communication

If something is worth measuring, the process of calculating these ITAM values should be well-documented, including the formulas used for each metric.

IT Managers should create a methods and procedures document that details all the benefit measurement processes.

They should then categorize each benefit type and develop a standard set of processes that will be used to measure that metric consistently.

Next the IT Manager should determine the frequency with which they will calculate and report each metric.

At Wanstor we suggest IT Managers develop an effective communication plan for appropriate stakeholders to report results. For example the CFO may only be interested in ITAM metrics that focus on areas of cost/budget reduction. The CIO however may desire a monthly dashboard that expresses ITAM benefits in all areas.

The important point here is to determine how and where you will maintain results.

Finally, consider auditing your processes. Unfortunately, ITAM teams can face a conflict of interest when measuring their own value. It can be beneficial to consult with internal auditors and request a formal review of process methodology and benefits calculations.

This will lend credibility to the metrics and can reduce or eliminate executives' skepticism about the findings.

However, as the ITAM discipline matures, its metrics and the audited benefits calculation methodology will, of necessity, evolve as well.

Additionally, ITAM's value metrics will have to be continuously tweaked and retuned to remain in alignment with the dynamic objectives of both IT and the business.

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.

Gartner peerinsights customers' choice 2018 ™

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

wanstor

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.

wanstor

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.

wanstor

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.

wanstor

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
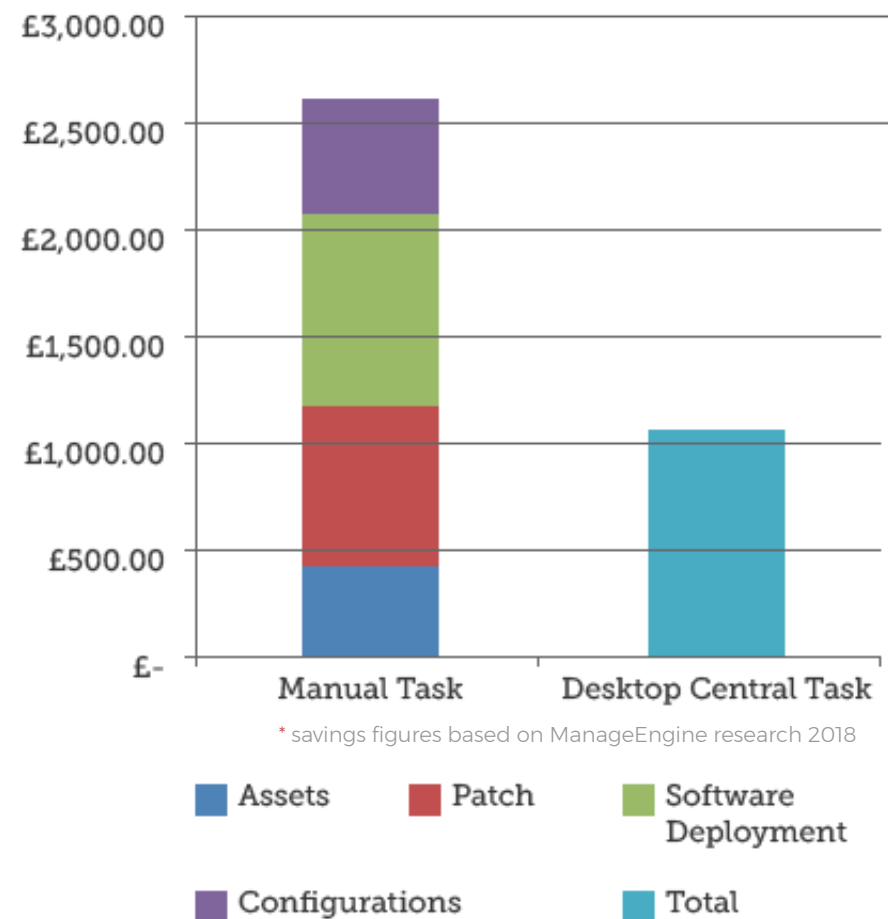
Manual task execution vs Desktop Central task execution

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 at **www.wanstor.com/manageengine-it-management-software.htm**

wanstor