Desktop Management

An Introductory Guide

wanstor

Contents

+ UNDERSTANDING DESKTOP MANAGEMENT
+ WHAT IS DESKTOP MANAGEMENT?
+ THE MODERN WORKPLACE
+ SECURITY, SECURITY, SECURITY
+ CORE FEATURES OF A DESKTOP MANAGEMENT SOLUTION
+ MANAGING A DIVERSE, MULTI-PLATFORM ENVIRONMENT
+ AUTOMATING ENFORCEMENT OF POLICIES AND RESTRICTIONS
+ IDENTIFYING COMPROMISED DEVICES PRE- AND POST-DEPLOYMENT
+ ADDRESSING LOST AND STOLEN DEVICES
+ PROTECTING CONTENT AND PROPRIETARY DATA
+ ENFORCING SECURITY POLICY COMPLIANCE
+ DEPLOYING AND SECURING APPS
+ APP DEPLOYMENT OPTIONS
+ PROTECTING APPS BY ENFORCING AUTHENTICATION AND SECURING DATA
+ PREVENTING UNAUTHORIZED ACCESS
+ AREAS TO THINK ABOUT BEFORE PURCHASING A DESKTOP MANAGEMENT SOLUTION
+ MANAGEENGINE DESKTOP CENTRAL OVERVIEW

wanstor

Understanding Desktop Management

IT teams have traditionally managed network security with firewalls, virtual private networks (VPNs), complex passwords, antivirus software, and computers imaged and deployed from within corporate walls.

However, today's devices generally fall outside the scope of most IT policies.

> **Most devices pose a significant threat to enterprise security and create complex problems for those in charge of device management**

Devices are part of everyday life and therefore part of everyday business. Such devices are no longer optional because they exist regardless of corporate policy, and for this reason, bring your own device (BYOD) policies have become commonplace.

Additionally an agile workforce depends on collaboration and communication across devices regardless of platform, ownership, and security.

What Is Desktop Management?

A quick search for desktop management brings up a range of interlinked phrases.

The two most common phrases are “desktop management“ and “unified endpoint management (UEM)”.

Between these terms they display hundreds of topics and multiple definitions, but they all agree that desktop management redefines end-user devices as “endpoints” and that the management of those endpoints is centralized, or unified, into a single application or a single application suite.

Endpoints are desktop computers, laptops, tablets, smartphones, wearables, sensors, and any other computing device used by an employee or guest to access network resources.

Network resources can range from connecting to an unsecured Wi-Fi access point to complete administrative access for IT staff members and everything in between for regular users, contractors, and guests.

However desktop management is much more than simply allowing or denying access to network resources; it’s single sign-on (SSO) management, user management, device management, device health checks, update management, resource management, device security, access control, and app delivery.

Using a desktop management solution can transform IT teams from chaos to calm by keeping network resources and business assets secure, while still providing the freedom users need to creatively solve business problems.

The logic behind desktop management

Both enterprise mobility and the adoption of BYOD programmes have forced business and not for profit organisations to investigate suitable IT management solutions for mobility and the mobile strategies they are looking to deploy.

Many organisations do not, however, want to support two or even three separate solutions in the workplace: one or two that cover laptops and desktops, the other for smartphones and tablets. What they are seeking is a solution that unifies end-users, endpoints, and everything in between.

An end-user's tendency to use one type of endpoint for a specific task doesn't rule out the possibility that a separate one could be used at any given time. No matter which endpoint is chosen, IT needs a way to keep track of it, and desktop management makes it possible to do so from the same platform.

Here are some of the most common platforms:

PC or laptop
91% of Internet users browse the Internet using these

Smartphone
80% of Internet users own a smartphone. Businesses can use a desktop management solution to deliver secure apps to devices that unify the user experience

The Modern Workplace

The days of users marching into an office, sitting down, logging into a desktop PC, and working all day from a single place are now in the past.

The modern workplace is here. Today's backpacks are loaded with laptop computers, tablets, and smartphones.

Many also carry e-book readers and hybrid laptops, and their devices may have different hardware manufacturers, running on separate platforms with distinct operating system versions.

> ## The modern workplace is not only mobile and diverse but also dynamic

Users are pushing the boundaries by asking for faster access, the ability to create larger documents, use different/more resources, and consume more data than ever before.

This paradigm shift has caught many companies and CIO's off guard, leaving IT staff and security professionals scrambling for answers and management options.

Security, security, security

A lack of strict device control often scares many business owners and executives away from BYOD programmes and away from a more mobile workforce.

IT security does not have to be a resource drain nor does it have to be a limiting factor in mobilizing users.

The good news is (despite all the doom mongers out there) that IT security is manageable.

It is true that if everyone left their mobile phone, computer, and tablet at the office, there would be far fewer security issues, but then, the workforce would suffer significant productivity setbacks.

> ## Users and unsecured devices are major threats for business and not-for-profit organisations

Malware, data leaks, and onboard cameras can have detrimental effects on an organisations reputation, intellectual property, and profits.

The solution is to impose security protocol in such a way that it's transparent to users, but powerful enough to protect a company's assets.

Desktop management solutions provide security across all devices, platforms, operating systems, apps, content, and their users in a consistent manner.

Quite often policies can be as strict or as relaxed as the organisation chooses. IT staff can apply broad policies to all users, while restricting others to a very high degree.

For example, apps that access corporate information can require a VPN secured connection to the company network — on a per-app basis.

This means a user's personal email operates outside of the secured apps' VPN and the data between the two apps never mix with each other.

This "containerization" protects the user's personal privacy and the company's proprietary data.

The need for a unified front

The real 'secret' to successful desktop management is the central or unified management feature. Any IT professional can tell you that trying to manage all endpoints with multiple tools is a big problem, for several reasons:

- There's the lack of competency with the use of several different tools. Too many tools lead to sprawl and costly mistakes because administrators can't train themselves on multiple, disparate systems.
- There's the upkeep of the tools themselves that can prove problematic. Can you see your staff efficiently updating and maintaining ten different security tools for managing user accounts and permissions?
- Having to do everything (provisioning, operating system maintenance, security, and decommissioning) manually leads to staffing bloat.

A desktop management solution can allow an IT department to perform more efficiently and allow management to significantly reduce IT staff numbers and lower the costs associated with endpoint maintenance.

Containerization can take many forms, from simple isolation to the setup of security boundaries or partitions between business applications and personal applications.

> In the strictest and most secure situations, a user's mobile phone will essentially become two devices; one business and one personal

The user's device isn't locked down in such a way as to prevent the user from enjoying social media, games, personal email, or personal messaging, but all corporate data and transmissions are separated by encrypted storage and encrypted communications.

Additionally, at the discretion of the company, a user's corporate data and apps may be removed at any time without affecting the user's device or personal applications.

Core features of a Desktop Management solution

Although terminology differs among desktop management vendors, functionality of the offerings remains relatively consistent. These core features are important to consider when selecting an endpoint management solution. The most advanced desktop management suites contain all five features:

- **MDM**: MDM includes endpoint life cycle management, endpoint on-boarding, provisioning, decommissioning, remote wipe, remote access, inventory, and operating system management
- **Mobile application management (MAM)**: MAM applies policies and controls to applications, including the ability to whitelist or blacklist applications, provide bulk distribution options, and make them available to enrolled devices and users via an Enterprise App Store
- **Content management:** Rules and policies apply to access to documents and other content resources from devices. These rules and policies are made right down to the individual file level and provide security and auditing trails for sensitive content. IT teams can set up Enterprise Document Catalogues to make the right content available to the right users

wanstor

- **Identity and access management**: Focused on endpoints and users, making sure that only trusted entities can gain secure access to corporate information. Service managed by identity management are app code signing, single sign-on (SSO), certificate management, and authentication. Context-based access improves security during authentication and authorisation by associating registered devices with user credentials and calculates risk based on a user's behavioural patterns to grant or to deny access to a resource

- **Containment**: System administrators can separate business apps and data from personal apps and data through password protected pre-configured apps or through application extensions, and prevent sensitive data from leaking externally

A Desktop Management Solution provides the following functions:

- **Provisioning:** Desktop Management suites configure users, devices, and applications for deployment and manage updates, upgrades, and decommissioning

- **Auditing, tracking, and reporting:** IT staff can accurately track endpoint inventory, audit devices, and produce reports on endpoint policy compliance

- **Loss prevention:** Endpoint theft, data access, endpoint lockdown and lockout, remote wipe, and application wrapping are a few of the security-focused functions available

- **Endpoint support:** Desktop management suites assist IT staff in troubleshooting problems through inventory, analytics, and remote-access activities

Managing a Diverse, Multi-Platform Environment

Managing a multi platform homogenous environment has some serious challenges associated with it.

In today's ever connected world the number of device possibilities approaches overwhelming without the right tools at the IT teams disposal.

> **Bring your own device (BYOD) programmes introduce multitudes of disparate device types into the corporate environment**

Then consider the diverse assortment of operating systems, operating system versions, and applications.

These factors combined give an entirely new meaning for the term *"device diversity."*

Just think of the entire range of security issues associated with those devices, operating systems, and applications.

The increased complexity that these devices bring to a corporate setting is enough to make even the most hardened IT Manager into a cold sweat.

The right desktop management solution should combine the management of users, devices, apps, and content with strong security to simplify a *"mobile"* approach.

IT teams can monitor for threats and automate compliance to maximize security without compromising the user experience.

Desktop management tools should collect device data and information and turn it into meaningful, manageable lists of tamed endpoints.

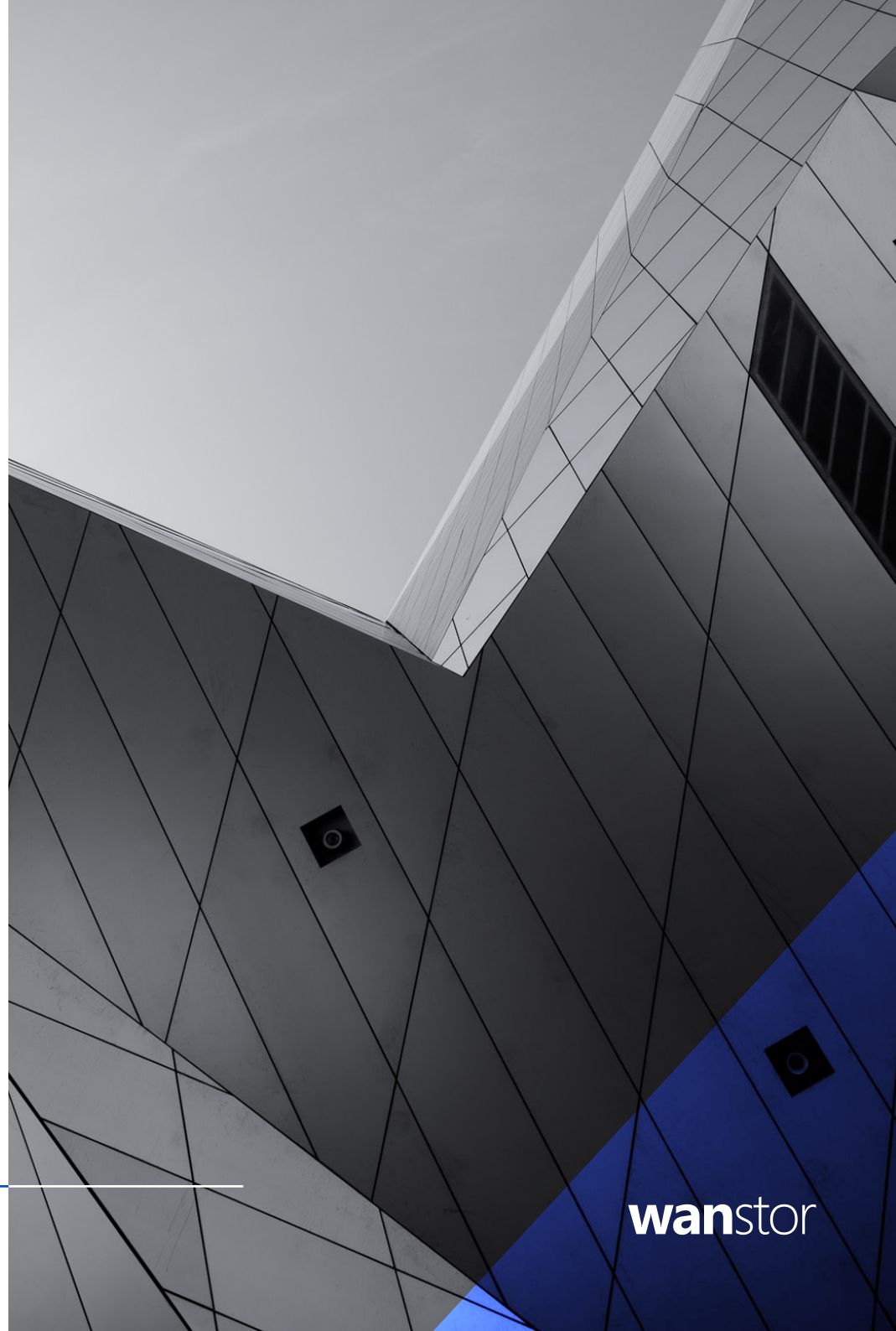
In short, desktop management tools should manage security, operating systems, patches, applications, and hardware for IT teams, and reduce the complexity of ever-expanding device diversity.

Automating Enforcement of Policies and Restrictions

System administrators can enforce policies and restrictions without ever touching an endpoint and do not require the endpoint to have corporate connectivity.

System administrators can modify passcodes and passcode restrictions, setup automatic app download, enforce operating system patches and updates, force all web traffic through a proxy server, and much more.

Endpoint management does not stop with enforcing security on employee devices, it should be extended to any enrolled device, such as those owned by guests and contractors.



wanstor

Identifying Compromised Devices before and after Deployment

Desktop management solutions should be able to detect and take action on jailbroken (iOS) and rooted (Android) devices.

Because they aren't considered secure, devices determined to be jailbroken or rooted during enrolment can be automatically quarantined via policy configuration, refusing its access to the corporate network.

> **A factory reset usually restores a device to its original condition allowing it to enrol as a managed endpoint**

If the desktop management system identifies a device as malware infected, the system administrator can prohibit it from completing its enrolment until the end-user has removed the infected app.

Administrators can configure policies to make sure automated steps are taken to address enrolled devices that have violated their corporate standards.

If system administrators choose to follow best practices, their users who jailbreak or root their devices after enrolment would trigger de-authorization in accordance with their corporate policy.
The same action would apply to devices infected with malware.

Subsequent actions are up to the system administrators, but their options consist of application-level wipe, container-level wipe, selective wipe, control removal, or a full factory wipe.

Several factors determine which action the desktop management console takes, such as device ownership, automated policy rules, and remote compliance rules. Administrators may also choose to respond manually.

Addressing Lost and Stolen Devices

With the capability to remotely wipe corporate data and enterprise apps, ManageEngine Desktop Central is fit to handle lost, stolen, and otherwise compromised endpoints. System administrators can also lock endpoints, shut down endpoints, and find an endpoint's last known location.

At Wanstor, we know that data breaches cost companies potentially millions of pounds in lost revenue, reputation damage, and lost data. Strict policy enforcement via a desktop management console can significantly reduce costs associated with endpoint loss by using remote wipe, remote lockout, remote shutdown, and geolocation. At Wanstor we recommend five practices for securing mobile devices:

- Implement a security policy
- Invest in physical security
- Never leave devices logged into networks, email, or websites
- Encrypt all data and secure networks
- Authenticate users and always know who has access

ManageEngine's Desktop Central addresses four out of five of these recommendations. Unfortunately, no desktop management solution can enforce physical security on endpoints.

Physical security requires an investment in security accessories, such as locking laptop cables, secure enclosures for tablet computers, and USB port locks.

It isn't enough for IT teams to write a security policy; they must enforce it by placing restrictions and policies onto the devices themselves.

Implementing a security policy means enforcing passcodes, timeout values, logout policies, and re-authentication rules.

System administrators can set timeout values on applications and devices so that idle applications and endpoints don't add to security risk.

Leaving an endpoint logged into email, a website, a corporate network, or to the device itself are all major security risks for an unattended endpoint.

Device and data encryption are desktop management controlled features. System administrators should elect to encrypt all corporate data in transit and at rest on the device.

Optionally, administrators can enforce full device encryption to secure an endpoint's data

Network, app, and device authentication are features that system administrators can use to verify that the user of an endpoint is legitimate.

Multi-factor authentication further ensures that the user is authorized to access corporate resources.

Physical security and encryption are two powerful deterrents to data loss and device theft.

Written corporate security policy should clearly identify physical security methods and encryption requirements.

Protecting Content and Proprietary Data

Users want to know that their personal data is private from corporate eyes or remote wipe events, and businesses want their data secure and separate from user data.

Without an endpoint management solution, the clear separation of personal and corporate data isn't possible to achieve.

For these reasons, many bring your own device (BYOD) programs fail

An effective BYOD program allows employees to work with technology that they own and feel comfortable using, while using it efficiently within their organisational role.

The problem is that users want the freedom to choose their own technology in the workplace, without extreme restrictions on personal functionality, spying, or the possibility of their data being wiped out by an overzealous administrator.

A heavy-handed approach to personal devices causes BYOD to fail. However, there is a solution that preserves and protects user data, yet also provides a comfortable security scenario for corporate data and apps: a device dual persona.

A dual persona separates a device into two zones: one preserving end-user privacy and the other protecting corporate, proprietary data.

A good endpoint management solution will provide a high level of security to corporate owned information on the endpoint — managing the data, apps, and security inside the corporate persona - giving employees the freedom to use their personal apps and data.

Containment

Containment is set up by the desktop management console to provide end-users with a separate security zone.

The container is a type of sandbox that only allows certain types of data to enter and leave. Only activities allowed by the endpoint management tool take place inside the container.

This is the main advantage to containerizing corporate data. System administrators can implement tight security policies without the possibility of cross-contamination with personal data.

A company can be as heavy-handed as necessary with the corporate container or containerized app without disruption to personal apps, data, or communications.

Containerized apps are the least intrusive approach to dual persona or to freedom in BYOD implementations.

Data stripping

The second, and least desirable approach to data separation is data stripping.

Data stripping is a security implementation that strips corporate data from common applications and redirects it to secure applications.

The reason that this approach is undesirable to many is that it presents the end-user with more steps than they'd normally have to take to undertake regular tasks.

For example, an employee uses the native mail client on a smartphone for personal and corporate email.

The user receives a business email but sees no content until the user opens the secure app to which the email has been directed.

Providing Secure Access to Sensitive Data

An endpoint management app as part of a desktop management system can protect sensitive data through enforced authentication and authorization controls. Each time an endpoint attempts a connection to a network resource, the endpoint manager authenticates the endpoint through its device ID. The end point manager then checks the device for security compliance and allows the device to connect if all policies pass.

User authentication (as shown in the figure), is the next layer of security for sensitive data access. The user's credentials must be authenticated and then check for authorization to access the resource.

If any part of device authentication or user authentication / authorization fails, the user can't access the resource. Knowing the difference between authentication and authorization is important. Authentication is the process of verifying one's credentials to a resource.

Authorization is the process of verifying that the resource allows the connection to complete. Authentication occurs first to verify credentials and then the resource checks for authorization. A user can have authentic credentials on a domain but not have resource authorization.

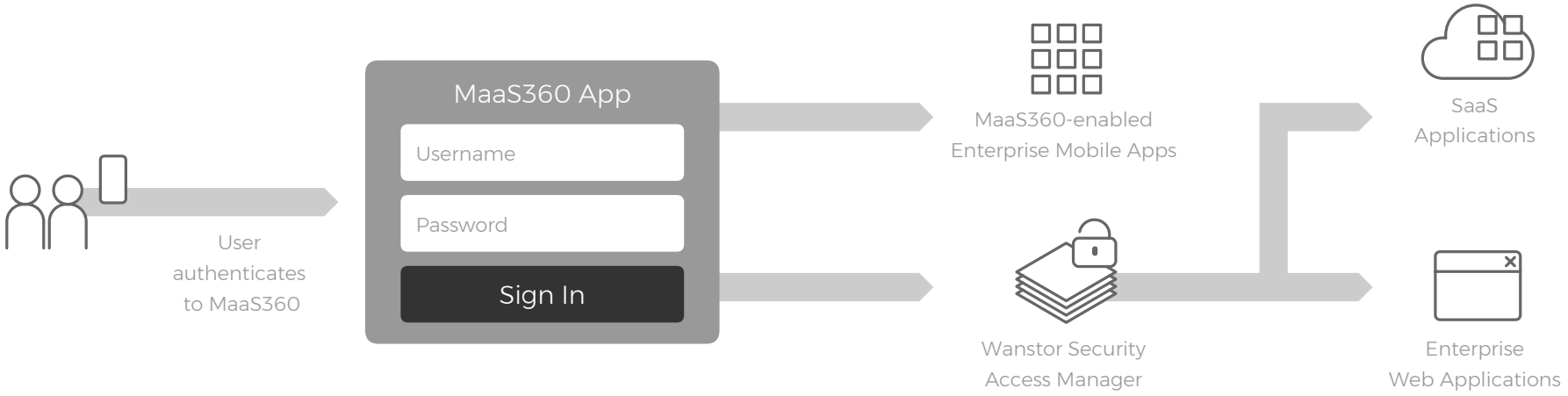


figure 1 : A UEM can provide secure access to resources without barriers to productivity and with minimal authentication friction

Enforcing Security Policy Compliance

There are two types of security policies: devices and users.

The desktop management solution is usually the business or not for profit organisations first line of defence for employees who remotely access corporate resources.

Endpoint management tools must strictly enforce this perimeter-based security to protect corporate assets, resources, secrets, and sensitive information. Allowing devices and users to enter an external portal into the network introduces risks. Security policy enforcement and compliance reduces those risks.

Device compliance begins with determining which types of devices IT teams will allow to enrol as endpoints. System administrators should decide how to handle devices that are jailbroken, rooted, or don't otherwise meet compliance restrictions for enrolment.

After enrolment, endpoints submit to regular compliance checks to remain updated with security fixes, operating system updates, patches, anti-malware signatures, and any updated security information from the network, such as new resource access.

The desktop management suite you choose should contain a mobile device management (MDM) module that handles the heavy lifting for device compliance and enforcement.

Securing Docs and Content Repositories

Content Management tools from a desktop management tool should provide the following features and benefits:

- **Enterprise document catalogue:** The document catalogue gives users a safer method of accessing and viewing documents
- **Document life cycle management:** Managing the entire document life cycle provides a more consistent and streamlined workflow approach for end-users
- **Compliance and enforcement:** Content Management protects documents and files. This module also prevents data leakage by restricting actions users can take regarding documents

The content management tool which is part of a desktop management solution should give administrators a central location from which to manage documents and to distribute documents.

Administrators can set expirations for documents to change access rules. To further protect sensitive information shared with users, administrators can restrict document sharing, printing, copying, and pasting outside of the secure container.

Deploying and Securing Apps

It isn't enough to secure documents or other network resources if the apps that connect to and use them aren't equally protected.

Application wrapping secures enterprise apps with a layer of protection afforded by corporate polices with zero reliance on developers for any code changes.

Pleasing your users with an Enterprise App Catalogue when managed properly, this behavioural trend can result in massive productivity boosts that benefit organisations at all levels.

However, when workers are left to their own devices, their apps can pose significant threats to enterprise network security.

This is largely due to non-secure data storage practices, malware infections, unauthorized access, lack of data or transmission encryption, and data leaks during syncing.

Millions of apps are right at the fingertips of end-users (most of which are unsafe for work and even personal use).

The enterprise app catalogue has answered the organisational need to make sure the right apps can be made available to the right users at any given time, while answering questions surrounding app security and approval for corporate use.

> **Enterprise app catalogues function much like public app stores, only they are managed by a company IT team**

All enterprise app catalogue apps will have been secured and pre-approved for corporate use from any compliant endpoint that is enrolled in the desktop management platform.

Users appreciate the enterprise app catalogue because it provides a central location where they can download and use apps without obtaining approvals or exceptions.

App Deployment Options

System administrators have several choices for deploying apps to enterprise users. The standard practice is to push a few selected apps to all endpoints so that users have a consistent experience across devices.

Enterprise app catalogues are optional but a strongly recommended option for users who would like a list of approved, secure apps that can be downloaded and used at will.

System administrators can selectively whitelist, blacklist, and require some apps from third parties, such as vendor app stores or manufacturer app stores.

Another option is to push optional apps to the endpoints. Users, however, do not always agree with the small list of required apps pushed onto their devices. Space and power constraints on a user's device are the two main issues users have against administrators pushing these optional apps.

The enterprise app catalogue contains a list of enterprise-built and enterprise-approved apps from which users may choose at will and on-demand as needed.

The vendor app store has the familiar look and feel that allows users to intuitively browse and select from all available apps, or those that have been packaged for specific groups or job functions.

Users need not worry about selecting any app from the app catalogue because the apps contained in it are secure, approved, and ready for deployment.

If an administrator finds that an app has a security problem, the administrator can remove it from endpoints and the catalogue. Apps presented in the enterprise app store also contain fewer superfluous functions and features than their vendor app store and third-party counterparts do.

They generally have a singular purpose for use in the workplace. Functions such as geolocation, push notifications, always on, and other power-draining, resource intensive features do not exist in these apps.

Apps delivered from the catalogue can also be maintained by system administrators. Your chosen desktop management tool should handle all updates, configurations, and optional features.

Protecting Apps by Enforcing Authentication and Securing Data

A good app protection tool in any desktop management solution should:

- Enforce data file protection to reduce data leakage risks
- Prevent access from compromised devices
- Use data leakage prevention (DLP) controls, such as no copy/paste or data backups
- Provide authentication before users access apps
- Set timeout values for single sign-on (SSO) across all apps
- Enforce on-device access controls
- Automatically delivers updates over-the-air (OTA) to all endpoints
- Wraps app in security code prior to deployment
- Containerizes apps to separate personal from business functions

At Wanstor we believe only a multi-layered security approach works for enterprises and devices that are constantly under pressure from advanced threats and ever-evolving malware exploits.

Preventing Unauthorized Access

When operating on a corporate network, versus working at home on their private systems, users do not always understand the risks they are exposing their company or not for profit organisation to.

For example, malware-infected devices can pose threats to corporate security.

After a malicious program or virus has infiltrated a complex network, it is very hard to remove completely. In dealing with Trojan horses and other delayed-release malware types, users can experience related infections for months.

Some malware programs allow the originator backdoor access into infected systems with elevated privileges, which can be extremely difficult to detect and to remove. The perimeter is the best place to stop malware by stopping it before it enters the network.

Desktop management solutions should monitor the devices requesting access to your network and work hand in hand with your network access control (NAC), to selectively allow or deny their connectivity based on several compromise checks.

Securing Access to Enterprise Resources

For today's end-users, gaining access to enterprise resources must be a quick and intuitive process; the inability to do so could be detrimental to productivity in countless scenarios.

Per-app or in-app VPN takes the pain and potential of secure app access. If a user opens the email app, the app initiates a VPN connection and will not operate until one is established.

The whole process is transparent to the user. The user opens the app, enters login credentials, and the rest is business as usual.

Device-level VPN also consumes a lot of bandwidth because every app the user opens during a VPN session sends its information over the VPN link and through your network.

Sure, the VPN encrypts the data, but there's a lot more data flowing through your VPN and your network than is necessary.

An app with built in VPN connectivity only sends its data to a VPN gateway and across the network. There is no mixing of traffic between business apps and personal apps.

What about apps connected directly to the corporate network?

You don't have a need for in-app VPN and the unnecessary traffic going outside and then back inside your network.

The app senses that it is inside your protected network and doesn't use the VPN, making app use and network use far more efficient.

Areas to think about before purchasing a desktop management solution

A good desktop management solution will combine mobile device management (MDM) and all other computing endpoints into a single application. To the desktop management tool, all devices are endpoints, and it manages them uniformly.

Finding the right solution to Meet the IT teams needs

Most business environments have many different types of devices at multiple patch levels and with varying degrees of security compliance.

The desktop management solution the IT team selects should bring these disparate devices under control for patching, malware protection, device-level security, app-level security, and user security.

ManageEngine's Desktop Central for example uniformly manages device, content, user, and app security across all devices, including laptops, desktops, smartphones, and tablets. Desktop Central allows IT teams to enrol and protect endpoints and their users all in one platform.

It is a desktop management suite that enables system administrators to place adequate restrictions on devices, apps, content, and data - while upholding privacy and giving the user enough space and resources to work in an unencumbered manner.

For example, when a user needs to open a protected network document, the app automatically and transparently opens an encrypted VPN connection to that resource for the user.

No user intervention is required - only a need to access the protected document from corporate storage. It also allows administrators to restrict access to apps from a corporate app catalogue.

Users may opt to install apps from this protected environment, ensuring that those apps are malware free and VPN-enabled. And desktop central supplies these protected apps to every enrolled device.

Cloud: Ease, Speed, and Savings

If the IT team has ever endured the process of procuring, deploying, imaging, managing, and paying for hardware, they will know that it's a slow, tedious, and costly process.

Cloud-based or Software as a Service (SaaS) offerings remove the complexity, the red tape, maintenance and expenses associated with on-premise hardware.

With a free, full production trial offering, no hardware purchase requirements, no scale-up or scale-back issues, no overprovisioning, no wasting of capacity, no customer data centre housing, and no hardware managing, it's easy to forget about the advantages of an on-premise solution.

Desktop Central can deliver recurring, no-impact software upgrades throughout the year. These updates deliver new functionality that's intended to enhance the customer experience.

No on-premise solution can offer that kind of uptime or smooth transitioning. In fact, most require ongoing maintenance by customers themselves to stay up to date with the latest technology.

Another major advantage to SaaS is that the IT team will never have to deal with obsolescence of hardware, platforms, or any software. They will never have to migrate from a legacy solution to a contemporary one.

Even if the IT Manager is in it for the financial savings, they should also consider ease and speed of cloud based desktop management services.

Delivering Consistent Support, Policies and Restrictions

Presently, most IT teams have one client management solution they use to configure policies and enforce restrictions on enterprise PCs and Macs.

They probably have another mobile device management (MDM) or enterprise mobility management (EMM) solution to manage your smartphones, tablets, and other endpoints such as ruggedized devices (not to mention their apps, docs, and data).

Plus they now have to find a whole new solution to manage the Internet of Things (IoT).

Juggling multiple solutions can be exhausting and seen as tedious for many IT professionals, they see it as losing precious time and incurring unnecessary costs. But what if the IT team could consolidate endpoint support, policy configuration, and restriction enforcement all from the same place?

As part of the definition of desktop management, you can. Desktop Central integrates, manages, and secures all endpoints, end users, and everything in between from a single platform. If the IT team want to restrict the use of external storage, they can easily distribute that rule to all applicable devices.

They do not have to swap from platform to platform to accomplish this. Instead they have one platform for all endpoints. Additionally the IT team can distribute the same authentication requirements across all devices.

Grant secure, seamless access to corporate resource. Make sure all devices meet security standards by either staying up to date on the latest software or maintaining the latest anti-malware signatures.

Update apps across all devices regardless of platform, operating system, or hardware vendor. Whilst, you'll enjoy the same level of visibility and support across all endpoints.

Positive End-User Experience

So, what does Desktop Central look like to the end-user? Think more native-like, and less learning curve.

Whether desktop central tools are used to send an email, chat with a colleague, create and share a doc, or download an enterprise app - the experience shouldn't seem any different from normal, everyday device use.

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.

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

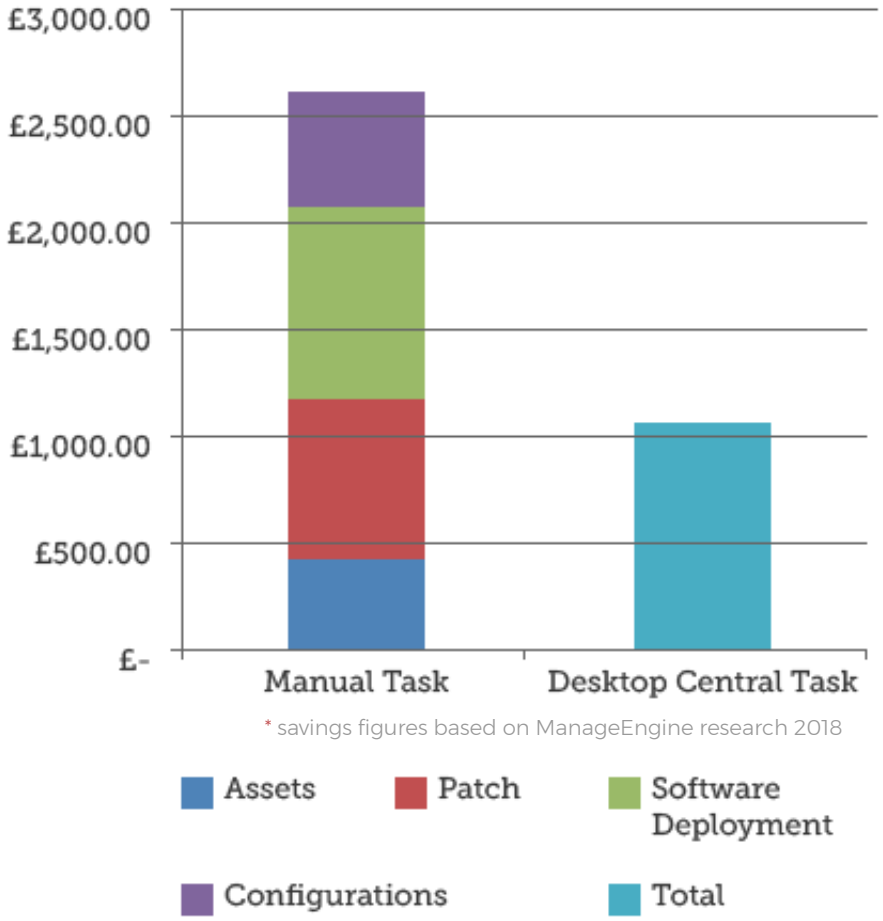
This example will demonstrate how Desktop Central saves IT teams, time, money and effort with a relevant and robust ROI calculation

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



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**

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

@wanstor.com

wanstor