Understanding Unified Endpoint Management (UEM)

WHITE PAPER

TABLE OF CONTENTS

Introduction

The enterprise landscape has undergone major changes. We have all been witnesses; seeing our enterprises evolve from a collection of immobile devices to devices that allow you to work from anywhere. While some of these resulted from years of experimentation, others emerged to prevent work interruptions in situations like the recent pandemic. The emergence of device management tools and the familiar end product- the Unified Endpoint Management (UEM) solution made the whole process easier.

1

Keeping pace with changing trends

We are all part of a dynamic technological world. The process initiated by the industrial revolution (more accurately, industry 1.0) starting in the 17th century saw many successors like industry 3.0, which gifted digitization and computers to the world.

Well, it didn't end there; with industry 4.0, digitization expanded further to higher realms, bringing to the scene many new implementations like the internet of things, cybersecurity, cloud computing, augmented reality and big data, among others.

Given below is a brief overview of the changes brought about by each of these revolutions:

Industry 1.0

- Mechanization, Steam power, weaving loom etc.
- Introduction of mechanical production facilities to the world, water and steam-powered machines helping workers in the mass production of goods.

Industry 2.0

- Mass production, assembly lines, electrical energy etc.
- Better known as "The technological revolution" with the emergence of new technological systems, most notably the introduction of superior electrical technology.

Industry 3.0

- Automation, computers, and electronics
- The advent of digitization with the introduction of transistors, microelectronics, and automation in the mid- 1990s.

Industry 4.0

- The dawn of cyber-physical systems, internet of things, networks. Centred around technologies like autonomous robots, simulation, system integration, internet of things, cybersecurity, cloud computing, additive manufacturing, augmented reality, big data etc.
- Modifications on the development of the third industrial revolution involving applications of information and communication technologies to industries.

Emerging device platforms

Devices are rapidly changing. Evolution can't be more related to an industry as it is linked to the smart-device industry. These devices have undergone many changes, restricted not just to physical modifications but also involving feature additions to keep pace with the changing trends.

Smartphones have changed to such a great extent that it is often difficult to establish connections between the ancient and modern forms merely based on appearance. We can also attribute this rapid change to the customer-centered nature of these industries.

With technological modifications and changing customer needs, smartphone industries are left with no option other than to modify these devices according to the fluctuating customer needs.

> “ Being customer-centred industries, the need to keep modifying these devices to meet customers' requirements always tops the list.

A shift towards device-friendly enterprises

Enterprises have grown far and wide with their openness to embrace variability. We have all reached a state where even the memory of our yesteryear workspace hostile to employee devices is hard for us to comprehend.

> “When we look back, it all began with the change brought about by Bring your own device (BYOD), giving employees the flexibility to use their own devices for work.

From work computers, it then expanded to include other devices like smartphones, tablets etc. And gradually, the line of separation between employee and enterprise devices faded even more.

Challenges in the workplace

With the world-changing day by day, we have also seen the workplace change from a group of immobile devices to devices we can carry around and work from literally anywhere.

Though these changes have made the way employees work easier, some factors need careful attention in an enterprise setting. Let's have a look at some of these challenges:

Deployment

Device deployment and management is indeed a challenging feat, especially if your organization comprises more than a few 100s endpoints. Configuring device settings and ensuring that each device meets the requirements of the employee job profile often becomes a demanding task.

Solving device issues

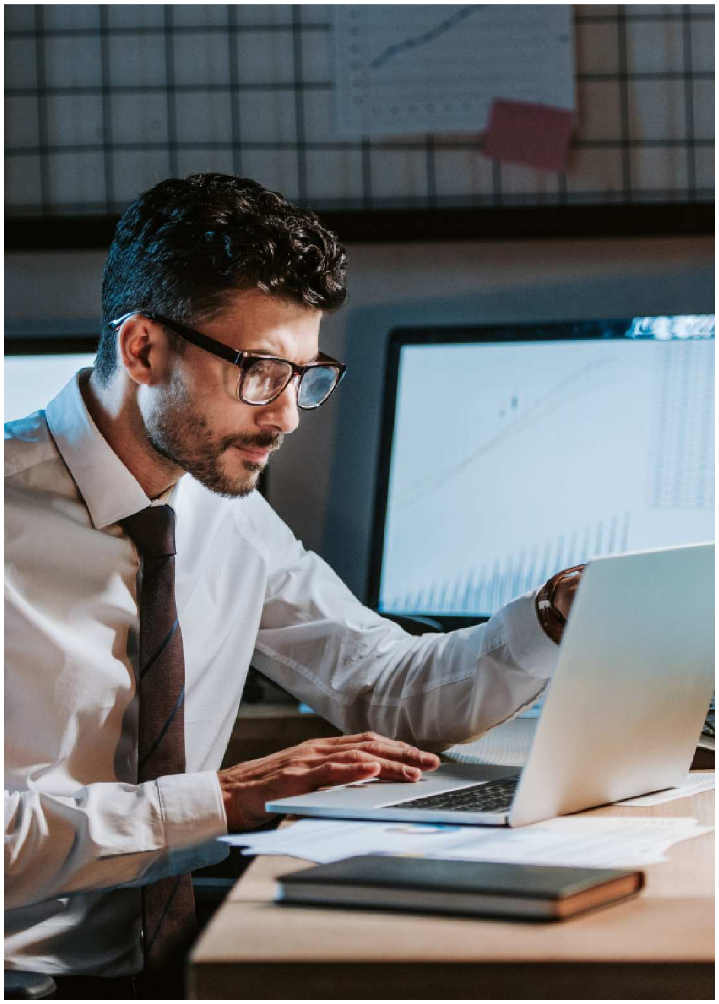
It's hard to imagine the IT sector without a large number of devices that employees work on daily. However, with devices emerges another major challenge – ensuring that your devices are always up and running, ensuring uninterrupted work. Under these circumstances, a provision to remotely troubleshoot device issues becomes all the more necessary.

Implementation of BYOD policies

One of the reasons why remote work, though difficult, wasn't impossible was due to the prevalence of trends like BYOD (Bring Your Own Device).

> “ BYOD implementation has erased the office boundaries, making it easier for the employees to work from their preferred location.

Its increased flexibility has also resulted in increased productivity and increased company morale. Despite these, it also brings some challenges to the workplace. Security risks, compliance issues, data removal and retrieval issues, vulnerability to malware, and inefficient password management are a few that need to be addressed.



IoT devices

IoT devices can best be described as a network of internet-connected devices collecting and transferring data across a network. They have been well known for giving constant feedback and facilitating better decision-making for businesses of all sizes. However, it also comes with its challenges that can be detrimental to the enterprises. Some of these aspects that need our attention include lack of encryption, brute forcing and the risk of default passwords, to mention a few.

Security

The role of security in enterprises does not need special emphasis. This pandemic period has witnessed the greatest peak in security incidents due to these tricky games played by malicious actors resulting in data breaches, ransomware attacks and many others. Enterprises need concrete security practices to shield themselves from all such incidents risking enterprise data.

Rapidly growing endpoints

New endpoints are being constantly added to the workspace. With technology penetrating all industrial sectors, we are no longer left with the option to completely cut them out of the enterprises. Hence, enterprises need to implement smart measures that ensure that these endpoints are not left out while ensuring enterprise data security.

2 The emergence of device management tools

As the gravity of challenges in the workplace began conquering greater realms, the focus shifted to effective tools capable of managing devices. This was the period of experimentation in the workplace, with new tools appearing and disappearing while others are becoming indispensable elements.

Client management tools (CMT) were among the earliest tools implemented for this purpose, succeeded by many others like MDM (Mobile Device Management), EMM (Enterprise Mobility Management) and ultimately the tool we all know – the UEM.

Let's have a closer look at Hexnode's UEM.

Hexnode UEM for device management

Unified endpoint management has become the all-encompassing solution capable of managing enterprise devices. Hexnode makes this process easier by its unified console single-handedly monitoring and controlling all device aspects. Let's have a closer look at how it manages each of these platforms:

Windows

Windows devices have always remained the most popular device in enterprises.

With these devices comprising such a great share, it's obvious how vital the management of these devices is in the enterprise.

Hexnode provides comprehensive device management capabilities for all your Windows devices in the enterprise. Starting with device enrollment, it extends further to effectively configure restrictions, device encryption, threat management, manage apps, prevent MDM removal, ensure network security, and a lot more.

Secure your enterprise devices

- Passwords
- BitLocker
- Microsoft defender

Configure device settings remotely

- Wi-fi
- VPN
- Email
- Exchange ActiveSync

Manage your device and your apps

- Restrictions
- Advanced restrictions
- App management
- Mandatory apps
- Blacklist/whitelist
- Custom Windows scripts

Secure device lockdown

- Single app kiosk
- Multi app kiosk

macOS

macOS is a series of graphical operating systems developed for Apple's Mac family of computers. It ranks as the second most widely used desktop OS after Microsoft Windows. Hexnode's macOS device management solution makes it easier for admins to manage endpoints, monitor, control and enforce policies on these devices while ensuring corporate data security.

Single console for managing all your apps

- Mandatory apps
- Blacklist/ whitelist
- App catalogue
- App configurations

Pre-configure your enterprise device

- Restrictions
- Advanced restrictions
- Wi-Fi
- VPN
- AD Asset binding
- Accounts

Configure device features remotely

- Deploy custom configurations
- Wallpaper
- Dock
- Setup Assistant
- Screensaver
- Screensaver
- AirPrint
- System Extensions
- Kernel Extensions
- Execute custom scripts

Securing your enterprise environment

- Passcode
- Privacy preferences
- Certificates
- Web content filtering
- OS updates
- Media Management
- Time Limits
- Smart Card authentication
- Firewall
- FileVault
- Login Window Preferences

Android

Android is undoubtedly the most popular mobile operating system globally, occupying around 70% of the mobile operating system market share worldwide.

Hexnode UEM offers robust Android management capabilities with policies tailored for app management, network security, update management, content management, remote view and control, mobile data management, personalization and a lot more. It also extends further to include Android enterprise to manage corporate and personal devices.

Securing Android devices in the enterprise

- Password
- Certificates
- Global HTTP Proxy
- Web content filtering
- OS Update
- Restrictions
- Advanced restrictions
- File management

Manage your apps from a single console

- Mandatory app
- Blacklist/whitelist
- App catalog
- App configurations
- App permissions
- Troubleshooting
- Hexnode App logs

Configure trusted networks

- Wi-Fi
- VPN
- APN

Configure device features remotely

- Wallpaper
- Boot/shutdown animation
- Periodic sync
- Accounts

Regulating enterprise data usage

- Network data usage management

Secure device lockdown mechanism

- Single App Kiosk
- Multi App Kiosk
- Digital Signage Display
- Website Kiosk
- Kiosk Screensaver

iOS

iOS is one of the most popular mobile operating systems powering many business devices, including iPhone, iPad and iPod touch.

Hexnode UEM makes it easier to manage iOS devices with their features like restrictions, app management, network security, OS updates, web content filtering, bypassing activation lock, remote view, mobile data management, personalization etc.

Manage all your apps effortlessly

- Mandatory apps
- Blacklist/ whitelist
- App catalog
- Web clips
- App notifications

Remotely configure all your enterprise accounts

- Email
- Exchange active sync
- CardDAV
- Calendar
- CalDAV
- Google account
- LDAP

Restrict device exposure to trusted networks

- Wi-Fi
- VPN
- Per-app VPN
- APN

Focusing on security in enterprises

- SCEP
- Certificates
- Global HTTP Proxy
- Web content filtering
- Managed domains
- Business container
- OS updates
- Passcode
- Restrictions
- Advanced restrictions

Regulating enterprise data usage

- Network usage rules

Remotely setup device configurations

- Deploy custom configurations
- Fonts
- Wallpaper
- Airprint
- Airplay
- Lock screen message
- Home screen layout

Secure device lockdown mechanism

- Single App
- Multi App
- Web App
- Autonomous Single App mode

Apple TV

The relatively new operating system- tvOS, was developed by Apple Inc. for the 2nd generation and later Apple TV digital media player. As more and more endpoints are being added, it becomes necessary to ensure that all these are managed effectively and do not pose a threat to the Enterprises.

Hexnode UEM supports a wide range of features like setting up Apple TV for conference room display, streaming Apple TV via Airplay, and more.

Personalize your device

- Conference room display
- Deploy custom configurations

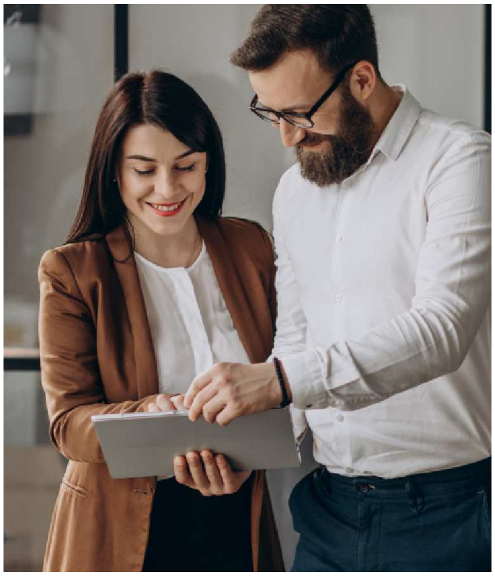
Features to ensure device security

- Airplay security
- Global HTTP proxy
- Certificates
- Configure Wi-Fi

Device lockdown mechanism

- Single App kiosk

Fire OS



FireOS is the name given to Amazon's operating system built on Android. Best described as the forked version of Android, apps running on Android devices are also supported on fire devices.

With Hexnode, you can easily manage enrollment, device restrictions, network configurations, app management, file distribution, mobile data management, kiosk etc. Some of its notable features include:

Manage all your apps from a single console

- Silent app installation
- Block or permit apps
- Update apps
- Setting up app permissions and configurations
- Downgrading applications
- App uninstallation
- Clearing application data or cache

Policies that ensure device security

- Multiple Kiosk modes
- Secure File management
- Network configurations
- Enforce device restrictions

Control your enterprise data usage

- Set data restrictions on Android
- Configuring network data usage management
- Manage data management on devices as per the needs

Conclusion

The pandemic has normalized practices like remote work and working from anywhere. It's a known fact that these practices are here to stay. However, this constantly evolving enterprise model demands equally competent device management measures. Hexnode has made device management a lot smoother by its features, ranging from security, app management, account management to the less covered aspects like data expense management, covering multiple platforms, all from a single console.