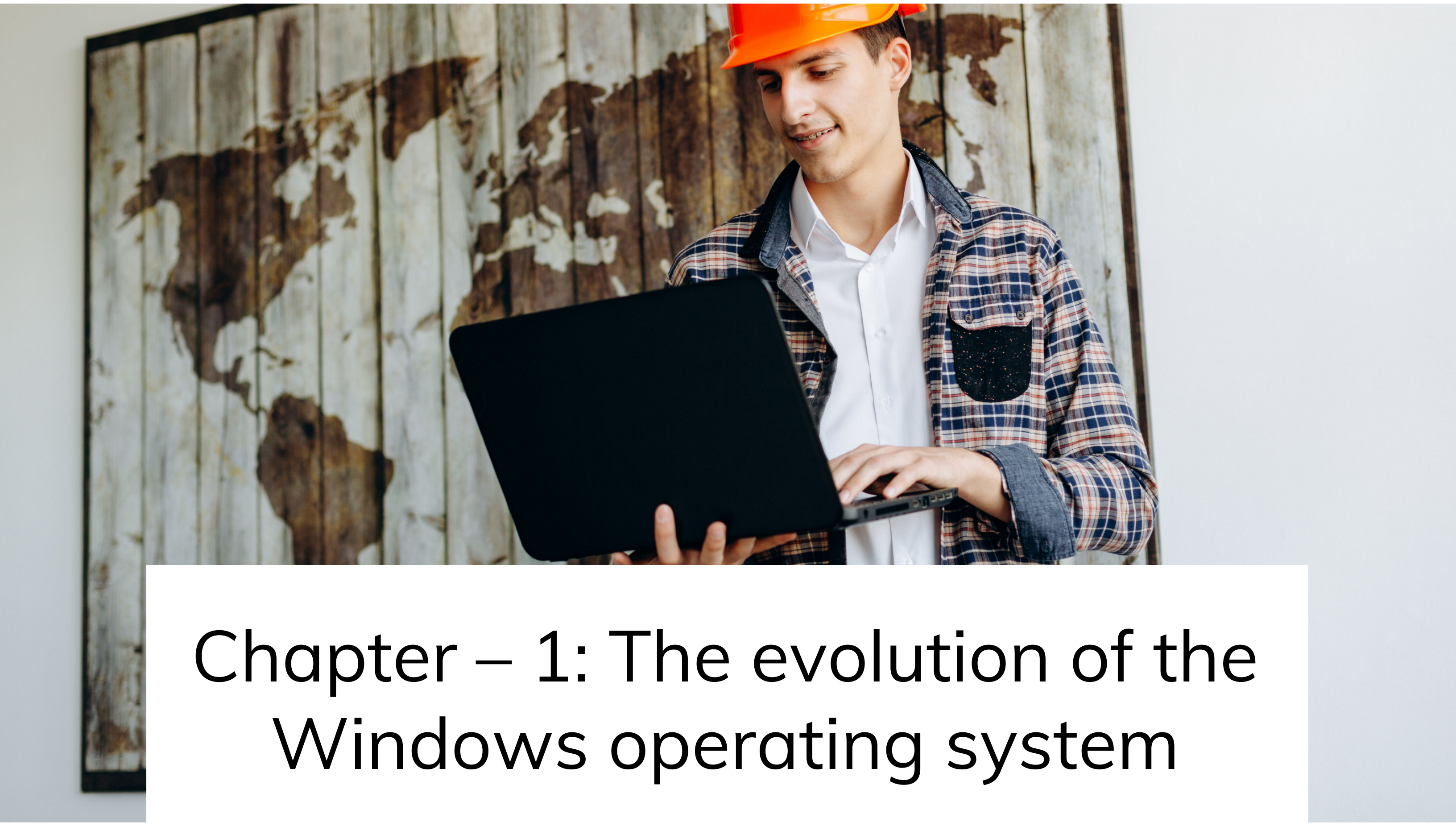
# The ultimate guide to Windows 10 PC management

WHITE PAPER

hexnode

# Table of Contents



# Chapter – 1: The evolution of the Windows operating system

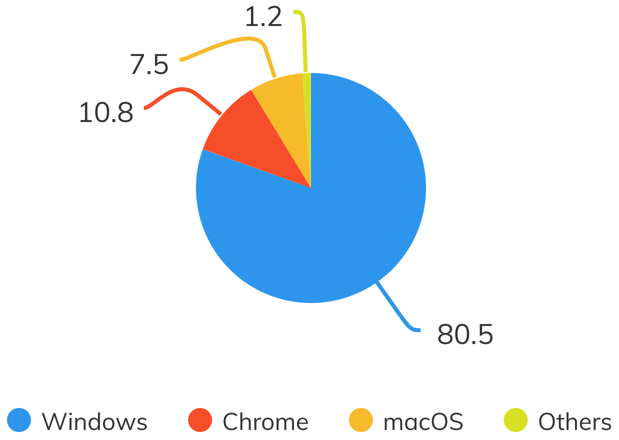
Windows 10 is widely praised as the most secure version of the Microsoft Windows operating system that has been ever released. All long its past experimental tries, Microsoft has always been dropping, altering, and adding features to its Windows OS with a vision to develop the best fit operating system for modern enterprise applications. However, Windows 10 is the closest point the tech giant has possibly reached towards accomplishing the so-called ideal enterprise model.

Windows 10 represents a radical overhaul for Microsoft with many important characteristic updates more closely aligned to enterprise-centric functions than its preceding versions, just as Microsoft dreamt its OS should have been. Not only that, but also the Windows 10 OS has been re-architected to enable better security and management flexibility. All these features together made this revolutionary OS the #1 choice for enterprise PCs.

# Why Windows remain the predominant operating system platform for organizations?

For ages now, Windows OS holds a commanding lead as the most popular desktop operating system. But another long-time contender with a distant second position, macOS, has been shifted to the third place when Chrome OS outsold the platform with a decent chunk in terms of market share the last year.

**Percent global market share for operating systems in 2020**



Source: IDC

Almost similar to this, when we take the enterprise usage, Windows OS holds an enormous market share. Modern organizations largely embrace Windows to offer a smooth enterprise mobility experience to their workforce. Windows PC is a part of so many offices across the globe and finds solutions for the broad challenges of the IT world. The noteworthy reason behind this ubiquitous popularity of Windows as the OS platform that laid the foundation for the PC landscape as we see it today is indeed its user-friendly UI. Open source operating systems like Linux still lags behind Windows, unable to ever compete with its usability features or even come closer to it. Furthermore, Windows have shaped up a surprisingly broader, stronger and expanding ecosystem with support to almost any piece of hardware and software. Having close collaboration with hardware partners, the OS embodies the base of a wide variety of devices ranging from desktops, consumer laptops, and professional PCs to mixed reality and gaming machines. Most developers build client-side applications primarily targeting Windows, and this extensive support makes it easy for organizations to deliver the tools their employees need. It is less likely to encounter compatibility issues with Windows while sharing files within the office or with other offices as it is long the standard operating system for businesses.

Security is another factor that gives Windows OS the head place. Nevertheless, Windows is known to resist security attacks better than macOS; it is still far better than open-source systems, which would take more time to recover from such cybersecurity incidents. Apple macOS, too, with its increased popularity, now came under the radar of cyber-attacks and are no longer malware resistant, which implies that they need not be always secure than Windows PCs.

Finally, Windows comes with negligible bugs and is quick to release fixes as and when needed. And if there is a question of the cost of ownership into the bargain, that would be the only area where Windows fails out to most open source operating systems. Still, Windows devices hold the upper hand for being economical than most versions of Mac devices.

# What makes Windows 10 an OS like no other?

Windows 10, which came in different versions catering to different use cases, unlike its predecessors, is the most popular and versatile Windows OS yet. Part of what makes Windows 10 appropriate for organizations include:

- Dynamic updates
- Windows Store and Business Store Portal
- Azure Active Directory features
- Universal apps and tools that work across all OS versions
- Provisioning packages for easy device set up

However, the most important update that came with Windows 10 is indeed the new management options. With Windows 10, organizations got the option to shift devices from traditional client management options to UEM solutions allowing IT pros to use the same tool to manage all the endpoints. And, of course, there will be many more updates on the way that will just keep providing organizations better opportunities to tighten security without compromising the end user experience with Windows 10.

# Chapter – 2: How Windows 10 PC changed the enterprise mobility landscape?

Iterations of Windows OS prior to Windows 10 never included any security features that proactively protected users, data and the broader enterprise from security threats. For this reason, Windows 10 is widely promoted for its security offerings such as encryption for local content, and enhanced authentication with multi factor credentials. But as with any OS that enjoys a massive user base, Windows 10 also is highly vulnerable to malicious attacks if not handled properly. Even though it holds up against several security woes, there are still some weaknesses the attackers can exploit. Another important concept at the center stage is the security vs. privacy concern. While organizations need to secure company resources and data on Windows 10 devices, with their superior enterprise mobility option, the end users look for a simple, high speed, flexible and consistent user experience. Attaining the right balance between security and privacy is not an easy task. The good thing is that the OS is equipped with a modern enterprise architecture that enables IT to evolve from a rigid PC-centric culture to a flexible mobility management model. This mobile and cloud first approach allow IT to maintain device compliance and ensure data security, providing improved user experience in parallel.

# PC management challenges for enterprise IT

The freedom and flexibility that mobile and cloud bring are significant that anyone can stay productive while on the move. But with this comes a fast-changing security and threat landscape. And this, in turn, requires enterprise IT teams to adapt to the changing user needs.

PC management has been traditionally complex and whatever possibly achieved with available tools was either too restrictive or too lenient. These commonly used tools with limited capabilities always fall short as the management requirements always had an ever-evolving nature which often included:

- Device deployment
- App distribution
- Patch management
- Inventory management
- Threat management and security
- OS update management
- Data protection
- Analytics and reporting

## How Windows 10 became a life-changer for PC management?

While PC management is generally a rough ride, Windows 10 OS has made an effort to lighten some of the processes with support to a new host of management features, thereby paving the way to a new mobility management paradigm.

Here are a few processes for which Windows 10 provides room for improvement:

1. Deployment – Device deployment is one of the most important challenges for enterprise IT. The prime concern before deploying Windows work devices would often be compatibility checking. But with Windows 10, compatibility is less of a matter of concern. In addition to this, Windows 10 eases the deployment process with support to new provisioning methods like ppkg enrollment.

2. App management – Windows 10 supports most of the modern applications across PCs, tablets, and even IoT devices, or the fact is that most applications are developed targeting this all-time popular OS.
3. Patch management – Windows 10 provides cumulative updates to make sure that the devices always stay up to date.
4. Security and threat management – Windows 10 has intelligent security capabilities with which the IT team can get insights into what's going on inside the device. It's quite easy to analyze the root causes and ensure protection in case of security issues. Windows Defender, the built-in threat management tool provides defense against external threats.
5. Data protection – Windows 10 has inbuilt support for data encryption tool BitLocker, which enables full volume encryption. Another tool called Microsoft Information Protection allows IT to enforce data policies to eliminate the chance of data breaches.
6. Identity management – Windows 10 has options to prevent access to the systems without proper authorization. Microsoft Passport to provide MFA, Windows Hello for business, SSO etc., are useful tools for basic level identity and access management.

Windows 10 just represent a major step forward for workplace technologies providing plenty of ways around the management challenges. IT just needs to find the right solution to solve the management challenges faced by their organization and create an ideal or not less than a near-perfect management model to address these challenges.

# Chapter – 3: How well does UEM really work for Windows 10 PC management?

Many traditional management tools have been out there to manage Windows devices, Microsoft Endpoint Configuration Manager (formerly SCCM), Group Policy, Active Directory, to name a few. PC management with these tools was one to one and completely manual, making the process difficult, unscalable and inflexible for the enterprise IT. For monitoring and remediating threat events, IT needs to rely on additional security tools. This siloed approach ends up only causing higher costs for the enterprise.

Modern trends of BYOD and Everywhere enterprise sometimes require deep granular control over devices and a light-touch privacy-focused management approach other times. While this may appear difficult with the traditional on-premises client management tool, with UEM, your organization can effortlessly support Windows 10 PC across all these management scenarios. UEM also unifies the management across a wide range of device types alongside Windows PC, thereby improving the overall ROI for your organization. Employees get empowered with working flexibility, whereas employers benefit from productivity enhancements while still maintaining the organizational security and manageability standards.

# Is it worthwhile to use UEM for Windows 10 management?

The major transformation that the UEM can bring for Windows 10 PC management is the shift from static legacy approaches to context-based strategies. With the traditional model, the devices remained fully controlled and well-configured only until the end users find out ways to tamper with the system settings. But with UEM, all the new management needs can be addressed, and any attack vectors can be prevented from anywhere, streamlining most of the traditional PC management responsibilities.

## GPO transitioning to UEM

Legacy Windows management was largely dependent on Group Policy Objects (GPO), which manages the user interaction with a system connected to LAN. This lacks the flexibility to manage non-network connected devices, and for organizations embracing BYOD, an additional management tool was inevitable, which added cost and complexity. UEM supports all the management scenarios and eases some of the hard ways with GPO though the features are not extensive as with GPO. In a domain admin's tool kit, GPO will still be a staple, but with a cloud-first, mobile-first model, UEM would be the better option for proactive management to avoid device downtime and maximize productivity.

## Windows 10 PC life cycle management with UEM

UEM offers deep manageability and security all along the device lifecycle.

1. Deployment: With UEM, you can provision Windows 10 devices as fully configured devices right out of the box through no-touch deployment options like Windows Autopilot. Self-contained provisioning packages could be created and used across similar use case device provisioning in bulk. There are many enrollment options to pre-configure the devices before enrollment and push out policies only after the end users enroll the device to UEM.
2. Configuration: Management settings and policies could be pushed to the devices based on the industrial use cases and level of management required. The pre-configured settings could be changed and updated as and when

needed. Policies could be automatically updated to device groups when they violate certain conditions using dynamic grouping and geofencing features.

3. Updating and troubleshooting: OS updates could be easily pushed, delayed, blocked or scheduled using UEM. Remote actions, remote view, and messaging features would come to use for device troubleshooting.
4. End of use: BYOD devices or devices issued by corporate for employees could be retired from management when an employee leaves the organization or if the device is found violating the compliance or security standards. Disenrollment is an easy process that could be done remotely by the IT administrator. Prior to deprovisioning, a complete wipe could also be done using the UEM itself.

# Key considerations for adopting a UEM solution for Windows 10 PC management

The right UEM can help organizations to reduce costs, boost security and improve end user experience. Although purchasing devices is an additional cost for organizations, a well-organized management model can offset the cost with improved business efficiency. A successful management strategy would be possible only if organizations decide upon certain factors before choosing the UEM solution.

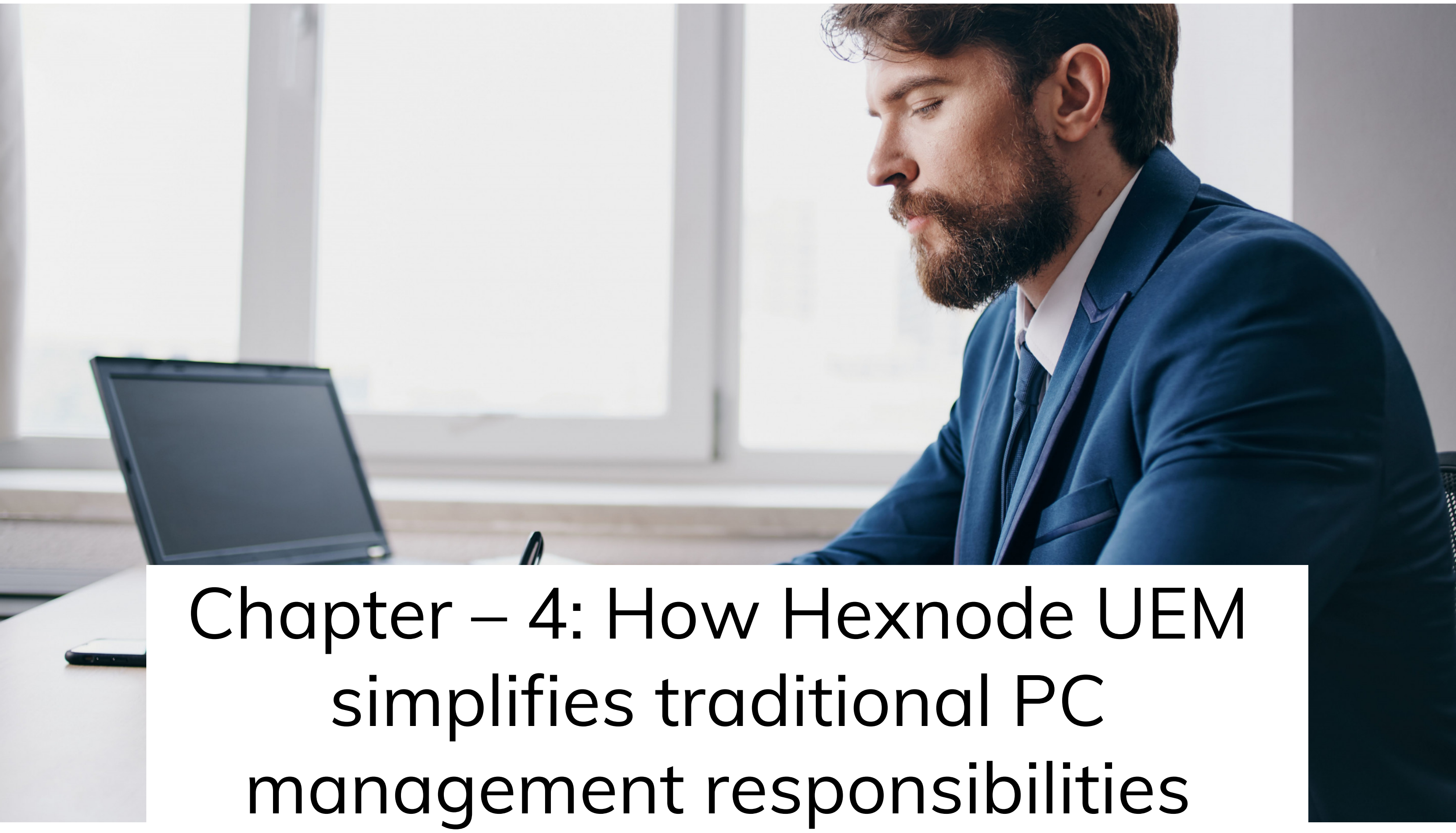
On-premises or cloud?

- Determining between on-premises and cloud administration is one of the primary steps. Organizations dealing with only managing network connected devices within the office would go for an on-premises approach. Almost all the client management tools are on-premises, and so organizations need not choose a UEM if they have to manage only domain-joined devices within the premises. However, for cloud-based management, adopting a UEM solution is a mandatory thing. Some UEMs provide support for both the on-premises and cloud deployment scenarios.
- Management model
  Decide on the level of management required for the intended devices:

1. Unmanaged – Devices require no IT control. End users will be able to change settings and make alterations - no need to enroll the device to UEM.
2. Somewhat managed – Only basic level management policies are needed. The device might be employee-owned. Applicable primarily for organizations supporting BYOD.
3. Fully managed – Advanced level management features and restrictions are required. The device might be corporate owned or corporate owned personally enabled.
4. Locked – Needs to be locked into one or a few apps and functionalities. The device might be purpose-built, sometimes shared, specific for a use case.

- Workforce type
  Consider what all types of workforce you need to support

1. Static worker – Works within the office
2. Mobile worker – Take work to home after office hours
3. Remote worker – Work from a location away from the office
4. Dynamic worker – Would be traveling most of the times and needs connectivity across diverse networks and devices



# Chapter – 4: How Hexnode UEM simplifies traditional PC management responsibilities

It is obvious that managing Windows PC from a centralized platform will save you in the long run. Hexnode UEM unifies the management of Windows 10 PC across the other endpoints in the enterprise and eases the transition from traditional PC lifecycle management to a modern IT management system.

## Hexnode vs. Traditional PC management tools

Organizations going with traditional PC management faces massive headaches during the onboarding and all along the management process. But companies having a device landscape highly reliant on different OS vendors like Apple, Google or Microsoft and the main computing devices include different form factors, like mobiles, tablets and PCs but not bound by legacy software dependencies, should have to depend on UEM tools.

When embraced with the right mindset, Hexnode UEM makes the management process simpler for organizations in various scenarios as compared to the legacy systems.

- Onboarding
  The enterprise IT should create a system image to deploy device settings with traditional client management tools. For this, each of the corporate devices should be manually accessed and configured individually. At the same time, Hexnode provides the option to easily onboard the device, and even the manual enrollment process is so simple that the end user himself can complete the setup without any assistance from the enterprise IT.
- Additional costs
  Using traditional client management tools for Windows 10 PC management ends up costing huge amounts of money for the organization. Additional data loss prevention, malware and security tools are to be installed on the device for ensured protection. But with Hexnode UEM, there are many security features which ensures complete protection for the device without the need for any added expenses. And a penny saved is a penny earned.
- Employee downtime and dependency on IT
  Working with traditional tools is too complex that the employees should completely depend on the enterprise IT for any changes to be made to the device. This would result in high employee downtime and impact their productivity. UEM processes are so simple that even a non-techy guy can easily do any process within no time.
- Unified device management
  Traditional management tools are designed solely for Windows and therefore won't offer extended support for non-Windows operating systems. Hexnode, on the other hand, is built from the ground way up for centralized management of all and any OS from a single platform.

- Task automation
  With traditional management tools, almost all processes are manual and complex. Hexnode helps automate most IT management tasks from device onboarding, app deployment, asset management, and location tracking to disenrollment.

# Future-proofing Windows 10 PC management with Hexnode

Hexnode was built for companies looking to take device management to the next level. This UEM tool helps you deliver a consistent, memorable, secure and user-centric experience across your devices every single time. Though Hexnode is a simple, surefire way to guarantee endpoint security, it's too easy to make a mistake or 10 when unfamiliarity and inexperience combine. So, knowing the product and product offerings well would help cut through these obstacles by taking the pressure off.

## Hexnode offerings for Windows 10 PC management

- Security management – Hexnode offers a unique baseline of endpoint protection features to detect, control and prevent security threats.

1. Comprehensive and real-time protection against software threats is ensured by checking the system requirements on target devices to run Microsoft Defender Application Guard.
2. BitLocker encryption settings are remotely configured for full disk encryption to the system drives, fixed data drives and removable drives attached to the PC.
3. Security restrictions like preventing the device from automatically pairing with other devices, mandating root certificates for provisional packages and preventing users from downloading beta updates.
4. Mandate device passwords and define complex password rules to make sure that the passwords used are never easy to guess.
5. Can restrict the users from removing the management profile from the device.

- Network configurations – For easy setup and ensured security, Hexnode allows admins to set up Wi-Fi, Email and Exchange ActiveSync accounts from the Hexnode portal itself, which eliminates the need for the user to set it up manually from the device end.
- Kiosk management – Hexnode helps to efficiently create a lockdown environment by restricting the device to a single app or a handful of apps.

- App management – Easy app distribution and silent app installation are salient features of Hexnode app management. In addition to this, there are options to mandate app installation and blacklist and whitelist apps to detect the presence of allowed or restricted apps. In all these cases, the device will be marked as non-compliant if a required app or allowed app is not absent or the presence of a prevented app is detected.
- Windows scripting – This is a bonus feature to automate that ultimate task automation option, scripting. Hexnode provides the option to remotely execute scripts to lessen the efforts and automate time consuming and repetitive IT jobs.
- Compliance management – Hexnode provides options to mark a device as non-compliant when certain standards defined by the admin are not met by the corporate devices.
- Automation – Dynamic groups can be created, and device policies could be applied to such groups to automatically push the restrictions or configurations to devices under the set conditions.
- Integrations – Hexnode integrates with AD, Azure AD, SCCM and many other programs to seamlessly migrate and manage devices added to these services.
- Remote management – Many actions like device wipe, lock and scan can be done remotely. Any action or policy could be pushed remotely. All applications can be distributed from a remote location. And overall, Hexnode eases the remote management of Windows 10 PCs from anywhere and everywhere.

For any organization, the move to UEM is appropriate for future-proof Windows 10 PC management. Hexnode is a compelling option for hassle-free endpoint management. Often the stress of getting started is enough to prevent anyone from getting started anything. With the ever-increasing adoption of Windows 10 PC by enterprises, today is just the right time for you to get started.