# Hexnode Unified Endpoint Management

An enterprise-trusted digital workspace management solution

### Key Benefits

- Comprehensive endpoint management support from a central console.
- Greater visibility and control over all your endpoints
- Scalable endpoint configuration and consistent user experience across endpoints.
- Supports multiple platforms and offers day-one support for latest releases of operating systems such as Android, iOS, Windows, Mac, tvOS, Fire OS.
- Seamless integration with existing architecture
- On-premises and SaaS deployment models
- Secure data across endpoints, networks and applications.
- Robust policy configuration and enforcement.
- Remote Troubleshooting
- Application and Content Management
- Identity and Access Management
- Threat detection and remediation
- Audits and Reports

With the recent proliferation of smartphones into workplaces, in addition to their inherent convenience, enterprises have introduced major changes in workspace behavior. With ‘consumerization of IT’ taking over the world, embracing new strategies like - Bring Your Own Device (BYOD), Corporate Owned Personally Enabled (COPE) has also become inevitable. As more and more devices keep adding on, maintaining the diverse ecosystem of devices afloat has become more demanding. Even though mobile endpoints brings-in several benefits' security remains a major concern for organizations around the globe. Since the inception of BYOD, COPE marked the next major advancement of mobile devices in the corporate infrastructure. COPE program enables end-users to choose corporate sanctioned devices for work and for their personal needs. Organizations can enforce policies to protect COPE devices at the app, data and device level without intruding into a user’s personal space.

Managing devices is no small feat, and the right choice of Unified Endpoint Management (UEM) solution is the key to making it work.

## Key Market Trends

Concurrently handling multiple devices is without question a tiering and a redundant task. Employees juggling with their personal and corporate devices at the workplace will not yield anything productive. This has led to the rapid adoption of personal devices at work and vice versa. However, this opens the door to a multitude of challenges like IT security issues, IT management cost hikes, etc.

The growing number of mobile users poses a greater risk to the organization. Every time they use their device outside the work environment, the chances of a data breach are considerably high. However, the sophistication in the technology has given rise to SaaS apps like UEM solutions that let the organization keep the data in secure storage on the cloud as opposed to the traditional on-prem network. The endpoint management SaaS apps also address the inconsistencies associated with user experience, cost management, security and IT support. These apps are even capable enough to make anywhere and anytime a productive working space for an employee. Organizations that fall back in embracing the new way of working often find themselves in the middle of unintended security breaches and severe productivity issues. A security solution like Hexnode lends a hand to systematically resolve such issues.

## What is Hexnode UEM?

Hexnode, an enterprise software division of Mitsogo Inc, is a global leader in Unified Endpoint Management. It is a comprehensive multi-platform device management solution that incorporates device, application, content, threat, telecom expense, and identity and access management capabilities to efficiently manage and effectively mobilize your organization's fleet of devices.

Hexnode Unified Endpoint Management goes beyond delivering the basic mobile and desktop management capabilities into the realm of universal endpoint protection and control to meticulously manage the entire fleet of mobile phones, laptops, tablets, desktops, wearables to IoT in your organization.

Hexnode helps the organization improve efficiency, increase productivity, save time and overhead costs of managing your corporate work devices.

### Why Hexnode UEM?

A Unified Endpoint Management solution that is as powerful as Hexnode simplifies user, device and security management of Enterprises across verticals.

- High Scalability: A single Hexnode server can support any number of devices as you wish.
- Software-as-a-Service delivery: Hexnode UEM is a SaaS app that facilitates storing your data in a secure location in the cloud. This relieves the organizations from setting up hardware or infrastructural components in the enterprise environment.
- Multi-Platform support: Whatever the device platform - Android, iOS, Windows, Mac, Apple TV, Fire OS, VR or IoT, it can all be managed using a unified management server.
- Multiple management options: Hexnode supports the management of personal BYO devices as well as enterprise-owned COPE devices.
- Robust tech assistance: Hexnode's technical support team will be at your disposal 24*5. You can resolve your queries in real-time through call, mail or chat.

# Core Features of Hexnode UEM

## Secure network configuration management

Hexnode lets you securely manage, monitor and troubleshoot corporate-owned and BYOD endpoints- desktops, laptops, smartphones, ruggedized devices, IoT across your organization from a central management console.

- Hexnode UEM integrates with Samsung Knox Mobile Enrollment (KME), Android Zero-touch Enrollment, Apple's Device Enrollment Program (DEP) to offer a no-touch, out-of-the-box onboarding experience to its users.
- Seamless and secure access to business data across endpoints.
- Comprehensive endpoint lifecycle management - enroll, provision, remotely manage and decommission endpoints, all from a "single pane of glass".
- Configure secure access to corporate resources, install public and enterprise apps, enforce security settings, prevent access to malicious websites and more with Hexnode.

## Easier Device Onboarding

Onboarding multi-platform devices in bulk is a tiresome task for IT managers. Hexnode offers a couple of alternatives that facilitate no-touch enrollment. This ensures device onboarding without any physical device contact. Android ROM, Android Zero-touch, Samsung KME and Apple DEP enrollments are some of the no-touch enrollment methods available in Hexnode. Moreover, organizations can level up and down the device enrollment security according to your needs. With the additional security options, organizations can enforce their users to verify their authenticity by signing in with their corporate credentials.

In addition to no-touch enrollment, Hexnode offers some minimal-touch enrollment options like Apple Configurator enrollment and Windows PPKG enrollment.

## Seamless administration

Managing and monitoring the devices enrolled in Hexnode is a piece of cake. IT managers can push any device management actions to any users or devices in Hexnode via a single click through the centralized web console. IT can even monitor and analyze the device's health through the UEM console. Hexnode is even equipped enough to let the admin check the live preview of the end-user device from the cloud console.

In conclusion, the entire feet of enterprise devices, irrespective of the management/enrollment type or platform, can be administered by a single/limit-ed number of IT managers from a server on the cloud with no fuss.

## Application Management

Hexnode's application management capabilities ensure seamless deployment and management of public, in-house (enterprise), and private apps across devices enrolled in your organization. You can distribute, update, track app behavior and manage the entire application lifecycle from a single console. In addition, you can

- Integrate your Apple Business Manager and Apple School Manager with Hexnode to seamlessly deliver VPP apps in bulk to your fleet of Apple devices.
- The VPP apps can be free or paid apps that are either the organization's internal private apps or the public apps available through the App Store.
- Enterprise app distribution and management for Android, iOS, macOS, tvOS and Windows devices.
- Distribute a unified app catalog to streamline app deployment on devices.
- Force apps to be mandatorily installed on devices to ensure that all the essential apps are available to the workforce on their devices
- Whitelist applications to ensure that the users can use only the apps approved by the organization. In contrast, you can also blacklist apps to prevent users from accessing non-productive apps.
- Proactive internet access controls to identify and impede the apps that exceed pre-configured bandwidth limits.
- Force apps to be uninstalled when the Hexnode is removed from devices. This ensures that the apps are available only on the devices managed via Hexnode.
- Force apps that are not deemed appropriate for the workforce to be uninstalled from work-managed devices.
- Allow specific apps to access business-critical data behind the firewall with per-app VPN.

- Limit access to Google Play Store, Microsoft Store, Apple's App Store to prevent users from installing non-productive apps. Prevent app installation from unknown sources, verify the credibility of the app prior to installation and more with Hexnode.

## Content Management

Hexnode's Content Management feature helps manage and secure content distribution to endpoints by leveraging policies at a granular level and enforcing robust authentication mechanisms to ensure that sensitive data is delivered securely over-the-air.

- Anytime, anywhere access to corporate data.
- Secure access to corporate emails, calendars, contacts, share corporate content from Office 365, Dropbox and more. With all the information at their fingertips, it can't get any easier to stay organized.
- Configure Data Loss Prevention (DLP) policies such as managed open-in, copy/paste, file-sharing restrictions.
- Remotely monitor and manage the files and folders on the work container of the enterprise deployed endpoints
- Set up the managed web and email domains to quickly identify and segregate work-critical data from the non-essentials and to regard them as a managed documents.
- Set up policies to control the flow of personal and corporate data between apps

## Identity and Access Management

Enable secure access to corporate content and resources with Hexnode UEM's powerful Access Management features. Seamlessly integrate corporate directories for user authentication, identity and access controls. Enforce policies with custom password rules, encryption and multi-factor authentication. Ensure adherence to corporate, industry, and federal regulations with curated compliance frameworks.

## Security Management

Hexnode implements robust security controls to protect data at rest, in motion and in use. Enhance employee productivity without compromising data security

to enable users to access corporate resources securely when and wherever they need them.

- Configure and apply data protection policies across Android, iOS, iPadOS macOS, tvOS, Fire OS and Windows, desktops and laptops.
- Lockdown your devices to only the applications, tools and settings that are critical to the workforce with kiosk mode
- Ensure secure access to corporate email, contacts and calendars on corporate-owned and personal devices.
- Containerize devices to create an encrypted compartment that lets you manage corporate apps and data and more.
- Configure password policies easily in compliance with organizational requirements.
- Perform seamless disc encryption on Mac and Windows devices to prevent unauthorized users from accessing sensitive corporate data on devices.
- Control the contents that can be viewed on the browsers with Web Content Filtering.
- Enforce encryption on the corporate devices to ensure corporate data protection from malicious attacks.
- Set up sophisticated Firewall, FileVault and threat management policies to protect the device from attacks, prevent unauthorized access and defend against virtual attacks.
- Schedule OS updates so that the device will stay immune to cyber-attacks. Also, you can delay the updates to buy enough time to check out the upgrades and make changes to your current flow if necessary.
- Set up an HTTP proxy policy to redirect all the traffic to and from the internet through a proxy server. This server filters out the corporate data and keeps it from reaching unauthorized personnel.

Hexnode offers proactive security controls in the event of a device being lost or stolen. If your device is missing and you have sensitive data on the device, you can remotely track the location of your devices in real-time, wipe the device to erase its contents, lock down your devices instantly, enable “Lost Mode” to prevent unauthorized users from accessing your device.

## Containerization / Work Profile Management

With Hexnode's support for BYOD Management, enterprises can now let employees bring in their own devices for work, increasing productivity and decreasing operational costs. Enterprises can separate and secure a part of users' personal devices for corporate use by deploying logical containers on devices.

- Deploy a work profile container on Android devices by enrolling your device in Android Enterprise (Android for Work) program. Push apps and install/uninstall apps silently, enforce app specific configurations and permissions, enforce data security settings on devices and more.
- Leverage Apple's management framework to seamlessly manage corporate apps and data separately from personal apps and data with Hexnode's iOS Business Container. The data exchange is defined using Managed Open-In, ensuring that the exchange occurs only between the managed apps
- Selective wipe ensures that only managed documents and apps are wiped from the personal device. This also enables to completely wipe all the corporate data from the devices, leaving space for no error.
- In addition, IT can prevent sharing of sensitive information outside of the work profile by enforcing copy/paste restrictions on devices.
- On Android, organizations can choose to deactivate the corporate data containers if the device does not adhere to the compliance policies specified by the organization..

## Kiosk Management

Dedicated device management is one of the strong suits of Hexnode. Kiosk mode on devices creates a restricted purpose-specific environment with minimal distractions and easy access to work resources. This is one of the simplest mechanisms by which organizations can boost productivity by shunting unnecessary distractions. In addition, Hexnode's kiosk management policies are very simple and easily configurable.

- Kiosk management for Android includes the single-app, multi-app and digital signage configurations. All apps, including enterprise, Managed Google Play, system, store and web apps, can be added in the kiosk mode. Note that you can also run apps in the background so that the apps won't be visible to the users.

- You can even customize the system features and the launcher settings on kiosk mode. Moreover, the web app kiosk policy lets you create a flawless web app experience for the users.

- Kiosk lockdown for iOS includes single app, multi-app, web app and autono-mous single app configurations. You can add enterprise, store, system, VPP and web apps to iOS devices. On launching the kiosk mode on the device, the users will be restricted from accessing all apps and features except the apps added in the kiosk mode along with the Settings and Phone apps.
- The Windows 10 devices enrolled in Hexnode can be locked in single or multi-app kiosk mode. The kiosk mode is supported on Windows 10 Pro, Enterprise and Education editions.
- Apple TV in Hexnode can be locked in such a way that the users can access only a single app running on the TV. Single app mode for Apple TV is available on supervised devices running tvOS. On associating the kiosk policy with the device, the app will be automatically launched on the device, and the user will be restricted from exiting the app.

## Telecom and Expense Management

The Telecom and Expense Management functionality offered by Hexnode allows businesses to efficiently track and monitor cellular and Wi-Fi data usage on devices. Remotely monitor and limit data usage on devices. Set up strict data usage restrictions for devices and apps. Monitor Wi-Fi, mobile and total data usage of individual devices and the data consumption details of applications installed on devices.

### Asset tracking

Hexnode assists organizations in gathering accurate real-time locations of the deployed devices. The UEM also auto-records the device location reports fetched at regular intervals of time. The technicians can avail these reports from the web portal anytime that they require it. Besides, even the most intrinsic device details like the installed apps, certificates, network connectivity, battery and memory usage, etc., can be monitored up close and recorded as reports in the web console.

Visit/learn more
www.hexnode.com

Sign up for a free trial
www.hexnode.com/mobile-device-man-age-ment/

Knowledge base
www.hexnode.com/mobile-device-man-age-ment/help/

## UEM Automation

Hexnode offers a number of ways to seamlessly automate the whole UEM experience for IT managers. Automation helps to untangle the already overcrowded work environment of the IT managers. Dynamic grouping is one such feature that enables organizations to automatically group devices that satisfy a specific criterion into a group. The group gets updated itself when new devices comply with the criteria or when the existing device breaks the criteria. The proactively associated policies will get automatically attached and detached from the devices as they move in and out of the group. Additionally, organiza-tions can employ geofencing to define the device's behavior inside and outside a secure environment.

With Hexnode, organizations can automatically send out alerts and notifications to the end-users and the technicians in case of a certain activity. Also, the auto-generated reports in Hexnode can be seamlessly distributed to end-users through the report scheduling feature.


Mitsogo Inc. United States (HQ) 111 Pine St #1225, San Francisco, CA 94111
Tel: Intl: +1-415-636-7555 Fax: +1-415-646-4151