How Hexnode UEM can help your enterprise with remote work

The COVID – 19 outbreak has the world working from their homes. The only cure we have right now is Social distancing and isolation. Most enterprises have already shifted their employees to work from their homes and the rest are getting prepared for it.
As an organization, you may have your concerns on allowing remote work for your employees like management, productivity, security, etc, but hopefully, this list of capabilities from Hexnode UEM for Companies considering the switch should put your mind at ease:

1. Easy Deployments

'Zero-Touch' device deployment solutions and no it is not a custom name for social distancing. You can monitor device health and status after enrolment via the Hexnode MDM portal.
Hexnode provides several open enrollment methods. The enrollment details are sent to the users via e-mail, as a message and QR code for bulk deployments.
Zero-touch enrolment methods include Apple business manager and Apple school manager, Android Zero Touch, Samsung Knox, and Android ROM/OEM enrollments.

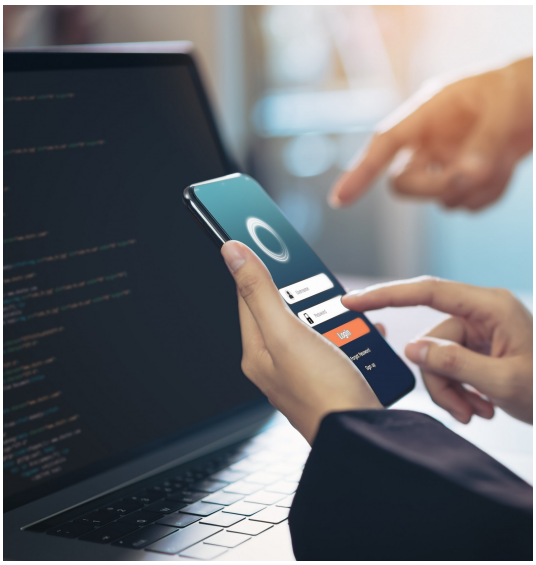
Enterprise enrollment methods include Android Enterprise, Active Directory, Azure AD, Self-Enrollment, Apple Configurator, and pre-approved enrollments.

Discover Zero-Touch Management

2. Pre-Configuration

Another nifty way to utilize Hexnode MDM is to pre-configure policies and push them to devices at the time of enrollment. Settings like mandatory applications, device restrictions and advanced restrictions, password policies, kiosk policies, application permissions, configurations and cataloging, security policies, and more are pre-configured are sent so that the devices are ready for work as soon as it is enrolled.

3. Restrictions



Hexnode UEM provides an unmatched array of restrictions and granular control over your devices like:

Mandating a passcode for securing enterprise data. The password quality can be set along with the frequency for updating this ensures that the corporate data always stays safe.

Button controls like Home, power, along with airplane mode, safe mode, lock screen shortcuts, home screen widgets, lock screen timeout and orientation can all be enabled and disabled from the Hexnode UEM portal.

Wi-Fi, Bluetooth, mobile data, tethering, and the ability to copy and paste between work and personal apps are frequently used to ensure higher security. GPS settings can be enabled or disabled along with the ability to set a mock location and the provision to force a location fetch.

And finally, blocking the ability to remove the MDM on the device can also be set up.

Beyond all this for certain supported devices advanced restrictions are available which includes: Microphone, Screen Capture, NFC, app installation and uninstallation, Airdrop, AirPlay, App stores, messages, calls, system bars, and their orientation, cellular network configurations, volume settings, clipboard settings, network configurations for wifi, portable hotspot.... the list is almost endless. As devices keep adding more features with updates, we are right with them to allow enterprises to block the unwanted updates so that a user-friendly update doesn't turn into an enterprise's nightmare.

Don't want to let them access more than the required applications? Lock it down with Hexnode's kiosk capabilities.

Hexnode MDM allows you to lock down your devices to a Single Application via the Single App kiosk mode and multiple applications via the Multi App kiosk mode. These lockdown features are available for iOS, iPadOS, Android, and Windows devices. Hexnode also provides options to restrict actions and device features during kiosk lockdown.

Besides these iOS and ipadOS devices have the ability to be locked down via the autonomous single app lockdown which can run just the selected application in the background without and interruptions. This feature can come in handy for schools conducting exams and employees working on just one application.

4. Location Tracking and Geo-Fencing

Hexnode UEM provides a very precise location tracking and geofencing capability. You can track your employees remotely. Hexnode also allows integrating the map API of your choice besides the default services. This can ensure that your employees are at home always staying safe and working.

The geofence policies can be used to monitor employees by setting up a fence around their homes. Leaving the fence will send an alert to you via email, portal alert, SMS, etc.

MDM location tracking – It's business, nothing personal

Check out a few industries that employees Hexnode's location tracking feature.

5. Remote actions

These include Remote view, remote control, remote wipe, etc. You can remotely view what your employees are viewing on their screens. This can help you keep tabs on ones that require attention. It can also come in handy for assistance and clearing and doubts or questions related to device operation.

6. Remote Control

The remote-control feature in Android devices (Android Enterprise, Knox devices, Rooted devices) can be used to remotely fix issues faced by the users as per requirement.
The remote wipe is an essential feature if you think someone is straying off guidelines with sensitive corporate data. You can remotely lock or wipe such data from their devices to ensure security.

7. Application, network management, Encryption

Hexnode's Data management and network management can be used to restrict and monitor where and how corporate data is used. In cases where the enterprise feels there

is a breach or possible security threat, remote actions can be leveraged to remove and secure the data.

Application management can aid in blacklisting unnecessary applications, the whitelisting of applications is also available on the Hexnode MDM portal. Whitelisting apps ensure that only the whitelisted applications are available for use all the other applications will be considered as blacklisted. Similarly, Whitelisting and Blacklisting of websites are also available. Besides ensuring that the employees are not distracted these policies also ensure that the corporate devices are not used for anything other than work.

Device encryption comes in handy if you want to secure your corporate data on devices used by the employees. Bitlocker for windows and File Vault for macOS devices are the most common examples.

The capabilities listed are just a highlight of the vast device management functions Hexnode has to offer. It's crucial that company's use these functionalities to manage their devices and allow employees to work from home so that we can overcome this hardship together as a community.