Hexnode - The perfect choice for Android device management

WHITE PAPER

hexnode

Table of Contents

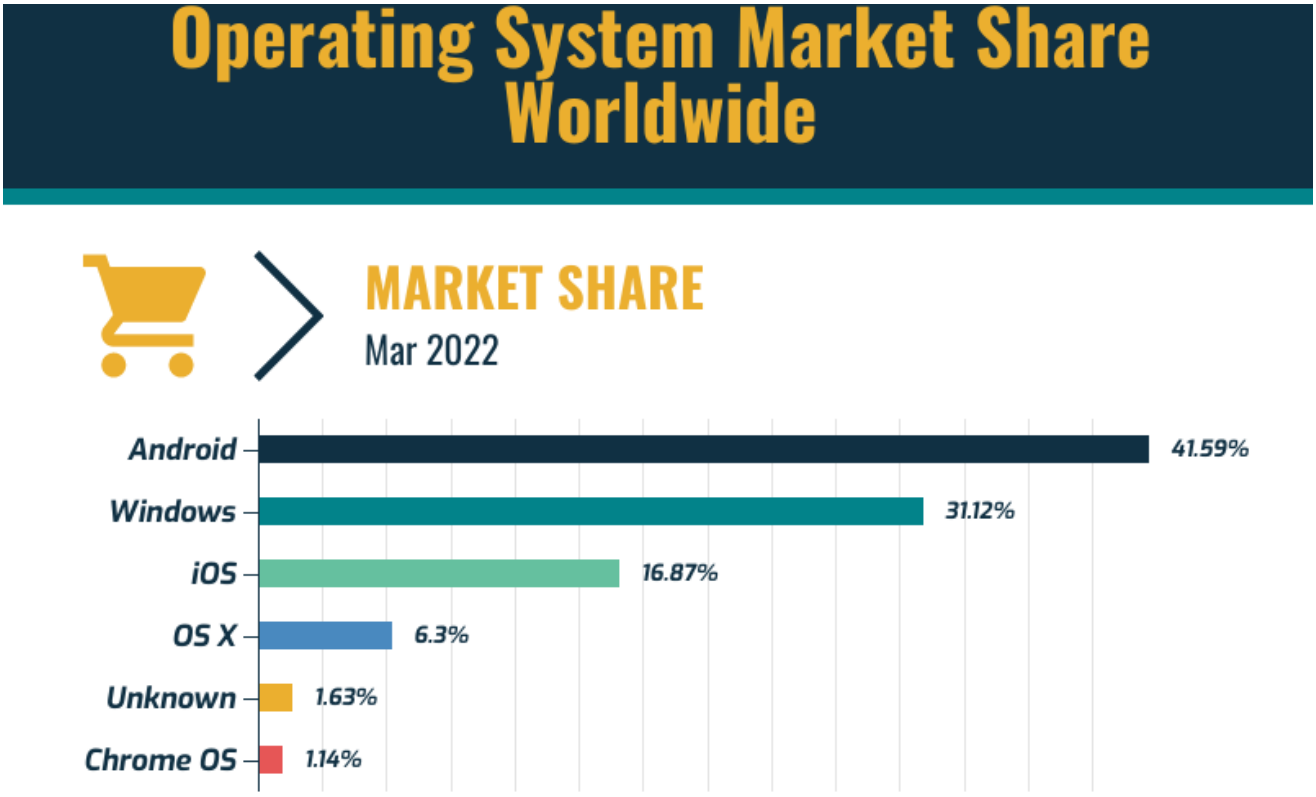
Chapter 1 - How UEM helps in managing Android device for Businesses?

With the ever-growing technology standards, businesses require a versatile solution for managing their endpoints. Relying on conventional device management methods poses the admin with several challenges.

According to 3rd Annual State of Enterprise Mobility Survey and Report conducted among IT administrators over 1500 companies across the globe, only 2% of IT admins feel that their MDM/UEM solution meets their expectations. The survey results indicate the need for better strategies in mobile device management. A solution that would proactively spot and fix the problems is the key to empowering frontline workers.

Ever since the advent of the UEM solution, device management has been a breeze. Over the past decade, MDM has advanced its management skills to all major platforms, thus evolving into Unified Endpoint Management (UEM). Hexnode is a key vendor in the UEM market. Hexnode has been featured in **KuppingerCole Leadership Compass**, **Forbes**, **9to5Mac**, **Cult of Mac** etc. The wall of fame is not merely limited to these but widespread across **Capterra**, **Gartner Peer Insights**, **Markets and Markets**, and more.

According to Operating System Market Share Worldwide, Android is the most dominant operating system, with a market share of 41.59% (As of March 2022).



However, Apple's iOS is still dominating the corporate world because of its increased security. But the introduction of Android Enterprise (formerly known as Android for Work) has paved the way for advanced Android device management. Android Enterprise features; in culmination with a UEM solution, can now meet the security aspects of a business.

This whitepaper addresses the need, importance and strategies for simplifying Android device management with Hexnode UEM.

Chapter 2 - Accelerate business productivity with Hexnode

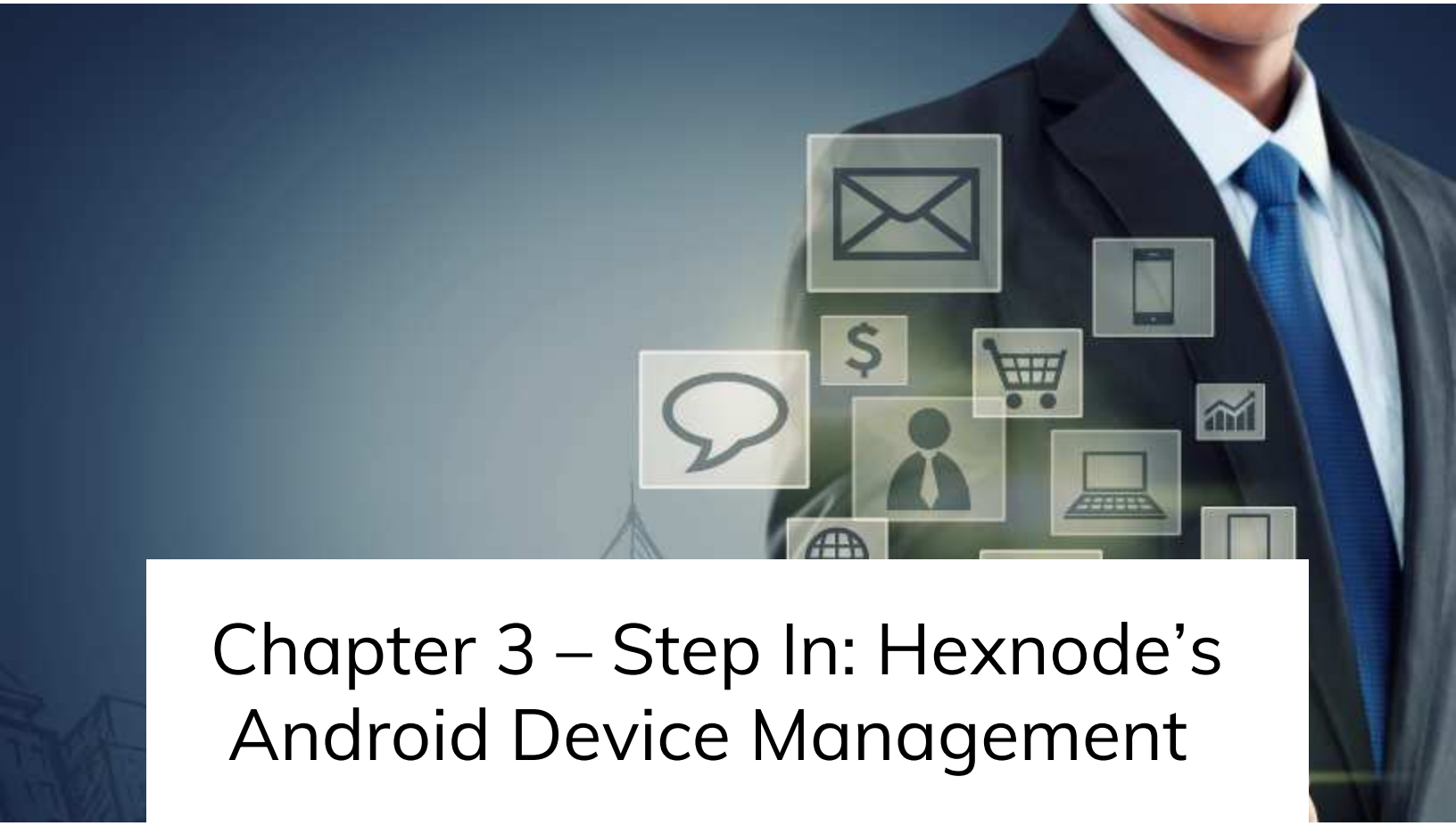
It’s been two years since the COVID-19 pandemic has hit the world, causing tremendous changes and revolutionizing the digital world. Since then, we have witnessed a shift from a normal office to a digital office. And, with the new norm being adopted globally, the days are gone when your users have logged into your network from their corporate devices. Instead, people are now even more comfortable accessing corporate resources from their personal devices, increasing the need for a mobile device management solution.

Today, enterprises are transitioning into clouds, and the trend of remote work has got a long way to go. According to a recent survey, a majority of the companies plan to introduce a hybrid model, where they are free to work either from the office or at home.

Now, the major question faced by the management is not how to manage these workforces but how to manage these complex devices? The two major concerns that IT administrators should address are security and privacy.

Malware, Phishing, Spoofing, SQL Injections, DNS Tunneling and other social engineering attacks can cause a major threat to enterprise security. The two channels used by the attackers to access the resources are the device with which you access them and the network on which the device is connected. Therefore, your organization must be prepared to adopt stronger network security with the aid of a perfect UEM solution like Hexnode. With the hybrid model being implemented, BYOD (Bring Your Device Management) is gaining more acceptance in the corporate world. Implementing a UEM solution on personal devices can cause the employees to double-check if their privacy is being compromised. An efficient device management solution can manage personal devices with keen policies and restrictions kept in place.

In 2022, the adoption rate of BYOD will be increasing at an alarming rate. Implementing a BYOD strategy could help in increasing employee productivity. Personal devices on their own don’t possess the ability to segregate between corporate and personal data. So, if a proper management strategy is not implemented, then BYOD could be a dead loss for the organization. Culminating both the privacy and security concerns paves the way for a better device management solution.



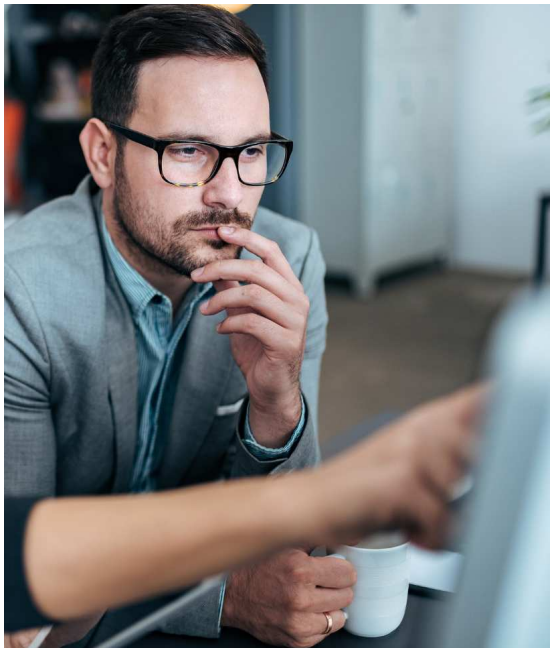
Chapter 3 – Step In: Hexnode's Android Device Management

Android being the dominant OS, the number of devices employed in enterprises is also high. The most common challenges faced by the IT admins on managing Android devices include:

- No proper mechanism for mass rollouts
- Trouble in managing OS updates
- Difficulty in rolling out Wi-Fi, VPN and Email profiles
- Separation of corporate and private data
- Data security

To overcome these challenges, IT admins need to rely on an efficient UEM solution, like Hexnode.
Hexnode's Android device management solution can be used to manage a plethora of endpoint devices, including mobile phones, TVs and soon even wearables. It allows you to remotely configure settings such as network, security, app deployment, content management, kiosks, and much more. In addition, integration with various tools and services helps in leveraging the existing features at a much faster rate.

Now, have a walk through the main features in Android,



Centralized management console

Hexnode provides a centralized management console where you can monitor and manage all your endpoint devices from a single pane. It provides holistic visibility of the entire fleet of devices. Therefore, Hexnode is a better choice, even if your organization needs to manage devices from multiple platforms. The web server used for the management of devices is generally addressed as the Hexnode UEM console. It has various management actions where you can gain insight into device details such as OS version, device management type, battery details and so on.

Device provisioning

OTA (Over the air) enrollment of devices simplifies the organization's asset management to a great extent. Hexnode provides you with zero-touch to minimal touch enrollment methods, where the corporate devices are ready for full-fledged deployment on a single switch. Various enrollment methods can be chosen based on the requirement of an organization. If you have to deploy the devices in bulk, go for Android's Zero Touch Enrollment (ZTE) or Samsung Knox Mobile Enrollment (KME). Else, you can go for a customized ROM enrollment method, where you can flash a custom ROM to the devices. Besides, Hexnode also provides you with the option to authenticate the enrollment using email, SMS or even QR code.

Although Android is the most omnipresent OS in the mobile world, its corporate acceptance is comparatively limited because of security issues. However, the introduction of the 'Android Enterprise' is a milestone in the Android revolution.

Remotely manage devices with actions and remote monitoring capabilities

Remote Actions are one-time management actions performed by the authorized personnel to execute a single command to devices in bulk. For instance, you can perform actions to instantly fetch the location of the devices, lock the device, clear the password, restart/power off the devices, remotely launch the app and much more. Hexnode's remote view and control feature come in handy under circumstances where the devices cannot be accessed physically. This helps the admins in resolving the issues with the real-time management of devices.

Managing devices via policies

Policies are the management profiles created from the centralized console, which can be used for setting up various restrictions across the devices, enforcing password rules to meet the corporate standard, helping the user to easily access corporate resources using Email/Wi-Fi/VPN profiles, block or allow access to set of applications, set up wallpapers and much more.
Depending upon the organization's use case, these policies can be associated with devices, users, groups and even domains.

Managing Apps and Content

The app requirements of an organization begin with the installation of the required applications. Hexnode's Android app management allows you to remotely install, update and remove apps from the devices. Besides, you can also block/allow access to a set of applications, set apps as mandatory apps, remotely configure app permissions/configurations and much more. The types of apps that can be managed via Hexnode include store, enterprise, web, and Managed Google Apps.
Remote deployment of the corporate files to Android devices can be made easier with Hexnode's content management features. It includes the provision to remotely share files like documents, images or videos to a specified device location. It also allows you to add files in kiosk mode, thus providing only limited content access to the users. Besides, you can also remotely move/copy/remove files from the device's internal storage.

Kiosk Management

In terms of kiosk management, Hexnode is the key player in the market, with the ability to manage the device settings even from the granular level to a more refined level. Hexnode's easy policy management allows to provision secure kiosks in minutes.

Hexnode's major kiosk management features for Android include locking down the apps in single app kiosk mode, multi-app kiosk modes with a customizable user interface, a web-based kiosk lockdown, where the device access is limited to the web pages approved by the organization, etc. It also aids in blacklisting/whitelisting the web pages as per the organization's demands. Apart from these, you can control the device volume, screen brightness, access to Wi-Fi while in kiosk mode, customization of the kiosk launcher settings, website kiosk settings and more.

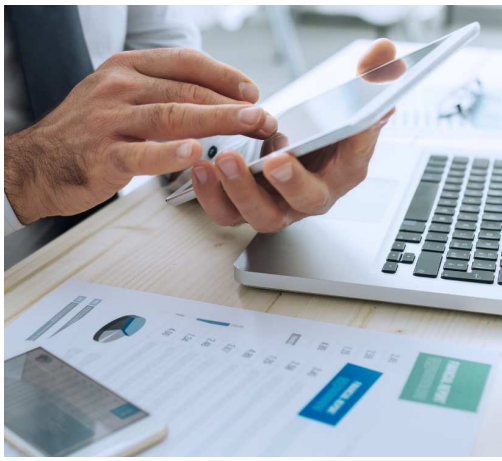
Web apps come into use in POS (Point Of Sale) devices, form filling and data collection devices etc. Hexnode's dedicated kiosk browsers can be used in situations like this, which helps in accessing more granular control over the device settings. Besides, Hexnode can also be used to configure digital signage, which has got utmost importance, as it helps in quickly transforming the ideas into virtual reality.

Location & Geofence

When the devices are being used for field works, the requirement to fetch the device locations at regular intervals becomes a major requirement among the IT administrators. Hexnode's location fetching features allows the admins to remotely fetch the real-time locations at regular intervals via policy, instantly fetch the device location via remote action, track the complete location traversed by the device, monitor the live location of the device from the dashboard, enforce location services on the devices, manual location check-in from the devices, preventing the devices from mocking the device location, Google Maps API integration, and so forth.

Geofence is a virtual-location service that creates a virtual fence around the required geographical region. This allows the admin to access the corporate resources as the devices enter/exit through the virtual boundary. Thus, preventing the device access to corporate resources from unauthorized locations.

Compliance check



Merely deploying the devices in bulk will not complete the device management. It should also have the provision to check if the device complies with the standards set up by the organization. With Hexnode, admins can ensure that the device complies with the requirements set such as application compliance, password compliance, device encryption and more. You can also ensure that the users/admins get notified if a device moves out of compliance.

Telecom & Expense Management

For organizations employing a remote workforce, the expenses incurred from network consumption can top the business's expenses. Telecom and expense management allows the administrators to effectively control the data usage on the devices, including the mobile data and the Wi-Fi data. With this, admins can limit the data usage for each of the devices. Apart from setting the limits, data usage can also be restricted if the consumption goes beyond the specified limit set by the organization. Besides, the admin can also be notified of the data consumption of the devices.

Integrations

Enterprise integrations with various tools and services ease up device management to a great extent. The integrations help in elevating device security, providing unparalleled management, maximizing flexibility, and improving mobility.
Hexnode has integrations with Samsung Knox, LG Gate, Kyocera, G Suite, Okta, AD, Azure AD and Zendesk. The integration with directory services such as AD, Azure AD and Okta helps in easier enrollment processes. It also facilitates syncing users and groups from their directory console to the MDM console. Integration with services like Microsoft and Okta also ensures Single Sign On (SSO) for the Hexnode technicians.
Furthermore, the introduction of OEMConfig apps revolutionized the device management industry. OEM vendors, in collaboration with UEM vendors, can together manage devices that support OEMConfig applications. AE's Managed App Configuration helps in setting up OEMConfig applications.

Monitoring and Reports

While applying the UEM policies, it should also be feasible for the admin to check and validate if all the devices are in place. Hexnode’s dashboard includes several widgets giving an overview of the total number of enrolled devices, users, applications deployed, type of applications, carrier info, geofence data, compliance criteria and more. It also includes an action history that logs all the activities registered within the Hexnode console.

The admins can also access the reports to analyze, monitor, and export the data. Hexnode provides you with options to generate the report instantly, or you can even schedule the report to multiple admins. The formats supported include CSV and PDF.

Chapter 4 – Android Enterprise – Marking a milestone in Android Revolution

The challenges and risks faced by organizations using consumer-grade mobile devices are high. Google's Android Enterprise can be leveraged to tackle these kinds of situations.

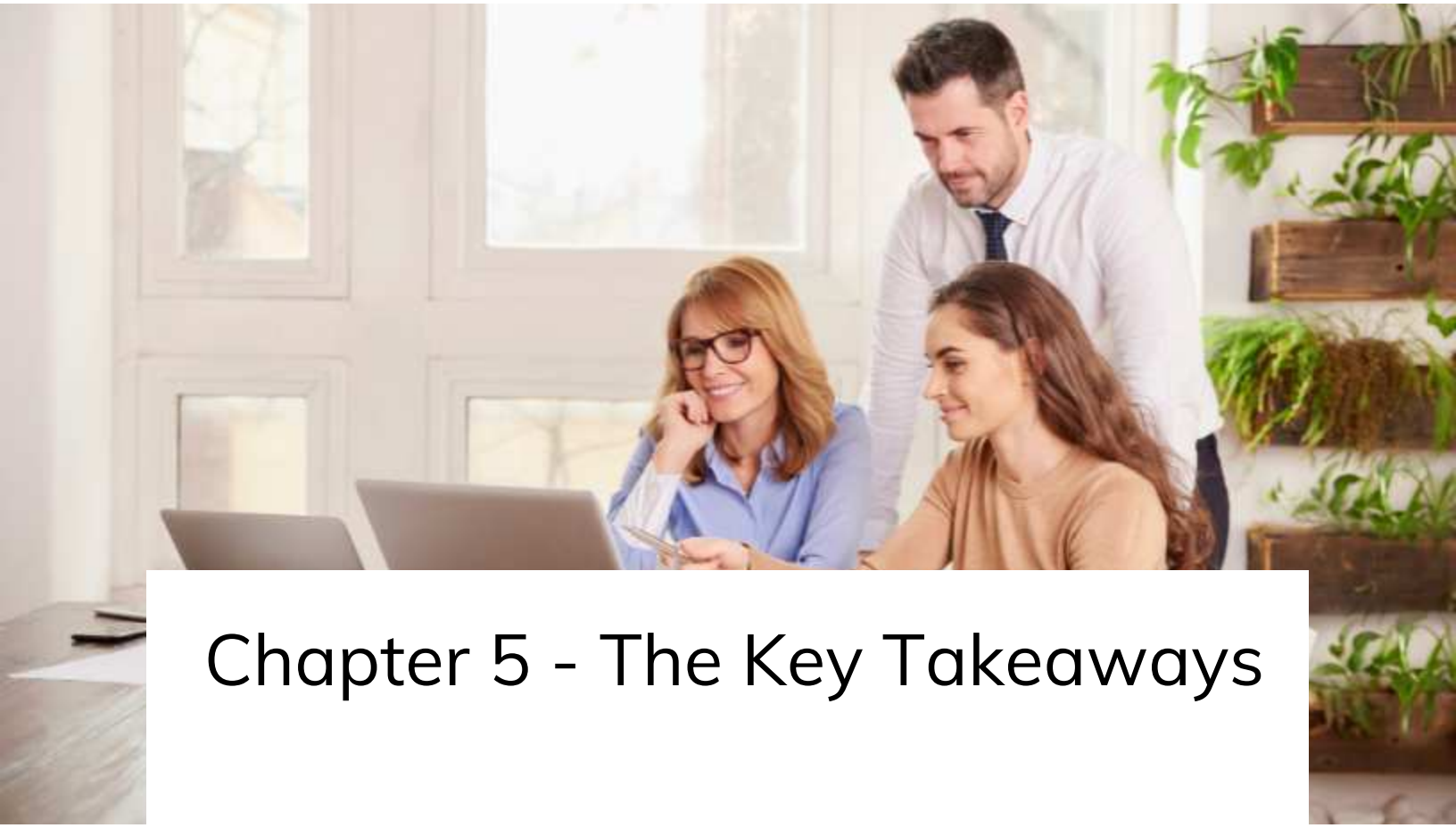
Situations may come when you want to access corporate resources while remote. Some situations may also demand to take your work device home. A Security breach is what awaits here. Since the enterprise data contains sensitive information, compromising them can lead to high financial losses and can even affect the credibility of the organization. Here’s where Android Enterprise comes into play.

Android Enterprise (AE) is a Google-led initiative that permits the use of Android devices in a work-specific environment. It uses a set of consistent APIs, which helps in the management of corporate deployed Android devices. The devices under AE can be enrolled in two different ways.

- **Profile Owner** – When personal devices are used to access the corporate data, they can be enrolled as Profile Owner in the Android Enterprise program. This creates a separate container for work data, thus preventing them from getting mixed with the personal data. However, the IT admin can access data only from the work container, thus leaving the personal data untouched. Thus, it can ensure security to the enterprise and privacy to the users.
- **Device Owner** – If the devices are owned by the organization, enrolling the devices in Device Owner mode ensures that the device is completely locked down for corporate purposes. So, complete control of the devices will be entrusted to the IT administrators. Thus, they can remotely lock/wipe the data if the device is compromised.

When the organization looks for BYOD management, they can deploy their devices in Profile Owner mode. And, if it's for Corporate Owned Business Only (COBO), they can go for Device Owner mode. Google's AE, in combination with a UEM solution like Hexnode, can be used for the granular device management of Android devices.

With Google's official announcement on the Device Admin deprecation, organizations are envisaging Android Enterprise as the near future of Android device management. Then comes the OEMConfig, a Google-defined standard that leverages app configuration to send Android device settings to applications developed by OEMs (original equipment manufacturers). The OEM vendors host the OEMConfig apps on the Google Play Store. This can be distributed to the target devices using a UEM solution. And, with the Managed App Configurations supported by the UEM solutions, the OEMConfig apps can configure the OEM settings while deploying them to the target entities. Thus, with the help of OEMs, UEMs can provide advanced control over Android Enterprise devices.



Chapter 5 - The Key Takeaways

When an organization deploys Hexnode UEM for Android device management, they can benefit from the following:

- Easier device onboarding.
- Ensures zero-day support for new OS versions using OEMConfig.
- Separate device management strategy for personal devices and corporate devices.
- Carry out instantaneous remote actions in bulk
- Restrict even the minute device settings via Hexnode’s restriction policy.
- Integration with Knox Platform for Enterprise (KPE) makes Samsung device management a breeze.
- Seamless app management by creating app groups, catalogs etc.
- Send app updates remotely over the air.
- Secure access to corporate data using network and security policies such as Wi-Fi, VPN, Email, Certificates etc.

- Reduce expense management by deploying data management policies.
- Cut down the device management time of the IT administrators.
- A remote work-friendly environment can be set up using BYOD and COBO policies.
- Enhanced end-user experience without affecting their work productivity.

Conclusion

The native device management strategies allow the administrators to manage a small business environment with fewer devices. However, if the devices to be managed are more or if the devices are widespread across various locations, then the conventional management strategies would be inadequate. To effectively manage your entire fleet of devices, businesses will have to integrate with Unified Endpoint Management Solutions, thus emphasizing a seamless workflow in their business. A robust UEM solution like Hexnode can cater to and meet your expectations, thus enhancing the productivity of your organization. In addition, it also provides adequate security without compromising employee privacy. Moreover, along with the technological advancements, Hexnode continues to add more and more features to Android device management, thus fulfilling the future requirements of your business.

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