Hexnode RMM solution

Automating remote monitoring and management of corporate endpoints

Key Takeaways

- Centralized management
- Personalize your endpoints to enhance user experience
- Schedule OS updates on devices remotely
- Get access to various reports and statistics about the managed devices
- Enforce strong passwords
- Prevent data leakage from lost/stolen devices
- Configure Wi-Fi and VPN settings
- Device compliance monitoring

A Remote Monitoring and Management (RMM) solution remotely manages and keeps an eye on business devices using locally installed agents. It enables you to manage users and endpoints from a single console. With Hexnode's RMM features, business networks will function efficiently and securely with well-managed remote monitoring.

The toolkit of an IT admin in an enterprise frequently includes RMM tools. They can obtain real-time information about the connected devices in the enterprise network. IT departments employ these tools to guarantee that remotely connected IT assets are standardized, performing at their best, and operating in compliance with business standards. In addition, RMM tools frequently include capabilities that enable IT professionals to monitor systems, assign tasks, track issues and automate maintenance chores.

With the combination of two essential tasks—remote monitoring and remote management—RMM software enables the enterprise to manage and secure its endpoints without interfering with the business's operations.

Features of Hexnode RMM solution

Hexnode provides the organization with access to various remote monitoring and management features that improve the efficiency of the IT infrastructure. The core features of Hexnode in assisting the remote monitoring and management solution is mentioned below.

Remote access and control

- Technicians can be given access to corporate devices using remote view and control feature so they may support and maintain them, examine usage data, and handle alerts.
- Admins may remotely lock devices, change owners, wipe passwords, and keep comprehensive control over corporate devices with Hexnode.
- These devices can be made more secure by enforcing a strict password policy, data loss protection methods, and network restrictions.
- Remote updates for the OS and apps are also made effortless.
- To increase security, specific devices can be restricted from joining an unmanaged Wi-Fi network.

Lost mode and wipe device actions

- Hexnode helps to remotely push wipe actions or enable lost mode for the managed devices, preventing unauthorized access to the corporate data they contain.
- Location history and live location tracking features of Hexnode help to locate a misplaced or lost device easily.
- Remotely configure appropriate lock screen messages to be shown on devices to assist finder in returning the device if it is lost or misplaced.
- Data leakage from lost or stolen devices can also be prevented by remotely locking or wiping the devices.

Wi-Fi and VPN configuration

- An enterprise can effectively save costs by turning off device functions including Wi-Fi tethering, data roaming, and application auto-sync.

- The corporate devices are not permitted to connect to an unmanaged Wi-Fi network so as to enhance security.
- Wi-Fi settings should be set up to allow users to join to the corporate network without being prompted for a password.
- Configurations for Wi-Fi and Virtual Private Networks (VPN) should use certificate-based authentication.
- Secure remote access to corporate resources can be achieved with Hexnode by configuring the VPN settings.
- Make sure corporate devices connect to secure gateways by configuring the APN settings.
- Configure a global HTTP proxy to ensure that all network connections go through it.

Password policies

- Implement secure password policies to safeguard the information stored on the devices.
- Define the standards for password complexity with length, special characters, timeout intervals, expiration dates, and retry restrictions.
- Any device that does not meet the requirements may be locked out or flagged as non-compliant.

File and application monitoring

- Hexnode enables organizations to manage and transmit content, including documents, applications, music, and videos to enrolled devices.
- Additionally, the storage location for the files can be specified.
- IT admins can set up app permissions and remotely push managed app configurations to have more control over the apps installed on the company devices.

- Admins can transmit files to a folder on the enrolled devices through the Hexnode portal.
- The Hexnode portal also allows for remote deletion of these files, which are also silently downloaded from the server.
- Users can be restricted from sharing data via Bluetooth and other file sharing methods.

Data usage monitoring

- Monitors the mobile data and Wi-Fi data usage.
- Through this, the company can set data use parameters, restrict the use of certain devices on a network, or disable network access altogether.
- When the data use exceeds the explicitly defined threshold, the user, the admin, or both the user and the admin will be notified depending on the setting configured.

Compliance checks

- Using Hexnode UEM, compliance settings can be defined to make sure that the enterprise endpoints adhere to the company policies.
- This will enable admins to keep an eye on the enrolled devices in real-time and make sure they always adhere to the regulations.
- The admin will be notified and the device will be flagged as non-compliant if it fails one of the pre-configured compliance parameters (such as installed app, geofence position, or encryption status).
- Monitoring password policy compliance, app compliance, and limiting Wi-Fi access to certain users are some of the effective compliance management tools offered by Hexnode.

Patch management

- Admins can maintain the security of the devices by remotely scheduling OS updates. Through this, all users would have access to the most recent system software.
- This offers companies the ability to check whether the endpoints on their networks are kept up to date, preventing potential security vulnerabilities from being exploited by attackers.
- Deploy policies specific to those devices by grouping devices based on their operating system.

Management of endpoints

- Hexnode assists IT managers in pushing user- and device-specific policies to enterprise devices that assist in app configuration and endpoint security.
- Identity certificates should be implemented to validate user access to corporate resources.
- Impose data usage restrictions across networks and applications of the organization.
- Only authorized employees should be able to access files that have been remotely deployed to devices.

Reports generation

- Hexnode produces reports on hardware, users, compliance, environments, locations, software, data management, and audit history.
- IT admins have the ability to view and export detailed report data as well as generate a variety of reports quickly.
- Admins can also receive scheduled reports through email on a regular basis.
- These reports generated can be exported as PDF or CSV files.

Visit/learn more

www.hexnode.com

Sign up for a free trial

www.hexnode.com/mobile-device-management/

Knowledge base

www.hexnode.com/mobile-device-management/help/

Benefits of using Hexnode RMM solution

Using Hexnode's Unified Endpoint Management solution, the enterprise can utilize advanced device management techniques to secure the devices from a centralized console. Enterprises can secure, monitor, and troubleshoot corporate endpoints from a centrally located console using extensive RMM features.

The main benefits of using Hexnode is mentioned below.

- Hexnode minimizes downtime by monitoring and resolving issues on enterprise devices. This will directly impact business productivity and increases overall profitability of the enterprise.
- Improved security by keeping check on vulnerabilities and thereby reducing the chances of security breaches.
- Enables the employer to restrict their usage of the company network for non-work-related purposes, thereby enhancing productivity.
- Reduced maintenance as it can rack and resolve IT issues of the enterprise.
- IT automation assist the deployment and configuration of apps and resources on managed devices. Dynamic groups, geofencing, and pushing custom script features are additional services provided by Hexnode.