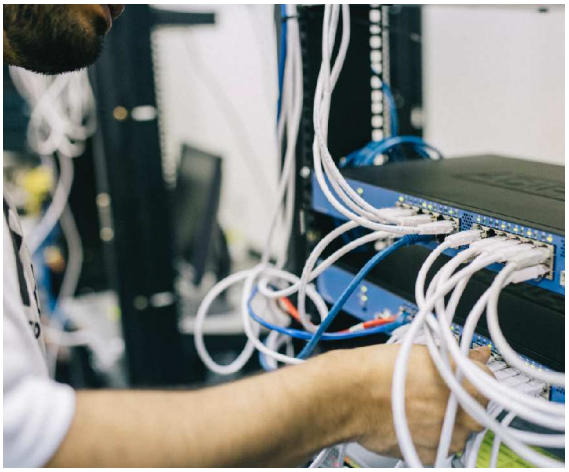
What is remote monitoring and management and how does it improve enterprise security?

hexnode

What is remote monitoring and management?

Remote monitoring and management (RMM) refer to the process of remotely maintaining and monitoring enterprise devices by means of locally installed agents. It lets you administer tasks and manage endpoints all from a centralized console.
Back in the old days, if your enterprise encountered system issues, or if you needed to check the status of your corporate devices, as an IT technician, you would travel to the company worksite and perform an on-premise system check. You'd perform the services as needed and bill the client only for the work done. Yes, it's pretty straightforward. And this method of providing IT support to your business is called the break-and-fix method of IT management.



Yep! On the outside, it paints a pretty cost-efficient picture. But, several drawbacks are hidden right beneath the surface. The biggest is the inability to monitor, manage and secure your corporate endpoints at remote locations. Your technicians cannot provide a reliable method to enforce Enterprise Security for your corporate devices. This is where Managed IT and the scope for a Remote Monitoring and Management solution comes in.

What does Remote Monitoring and Management do?

An RMM software combines two key activities – remote monitoring and remote management – letting you manage and secure corporate endpoints, without ever needing to set foot on the company premise.

What is Remote Monitoring?

Remote monitoring involves observing and recording the network activity of all your users from a centralized point. It monitors the endpoints managed by your enterprise 24/7 with the help of compliance checks and reports.

What is Remote Management?

Remote Management lets you remotely control and administer enterprise operations from a centralized location. It collectively combines all the practices dealing with controlling and managing endpoints, including setting up devices over the air, troubleshooting issues, and protecting business data from malicious attacks.

Together, Remote Monitoring and Management software enables you to control your business IT operations and lets you provide:

- Continuous Monitoring and Reporting
- Management of Mobile Devices
- Enterprise Security Management
- Seamless Onboarding and Integration
- Automated Software Updates and Patches

What are the benefits of using Remote Monitoring and Management software?

Minimize downtime

Gone are the days when you'd have a technician come over to your office to resolve your IT issues. With RMM software, your technician can track the health and status of all your enterprise devices from a remote location. This lets them identify and resolve issues with minimum downtime.

Provide better security

Reduce the risk of malware attacks and data breaches. Using Remote Monitoring and Management software, you can set up security policies and monitor your endpoints 24/7 to prevent potential threats from entering your system.

Reduce maintenance and capital expenses

As opposed to a pay-to-fix model of traditional IT service, with RMM, you can track and resolve your enterprise IT issues on a subscription model. This reduces the overall cost and capital expenses incurred by your business.

Increase productivity

By reducing system downtime with continuous reporting and monitoring and constantly updating your system to the latest software updates and patches, your employees can work more hours without interruptions or system failures. This improves your business's overall productivity.

Remote Monitoring and Management with Hexnode

Hexnode's Unified Endpoint Management (UEM) solution equips your enterprise with a suite of Remote Monitoring and Management features to strengthen your IT management capabilities.

Continuous Monitoring and Reporting

Hexnode's RMM strategies help you gain insight into your enterprise devices' health and status and provide reports on the users' network and systems.

Compliance Checks

With Hexnode, you can define compliance settings to ensure that your endpoints conform to corporate regulations. You can also set the level of security required by your enterprise. If the devices fail to meet the requirements, Hexnode UEM will flag them as non-compliant.

Generate Reports

Hexnode generates reports on devices, users, compliance, locations, applications, data management and audit history. You can view and manage reports instantly or configure them to be generated at a scheduled time and sent to your email. You can also export reports from Hexnode in the form of PDF or CSV files.

Remote Access Tools

Hexnode's Remote-view and Remote-control features let you resolve your client's technical issues in real-time and ease the process of troubleshooting devices.

Location Tracking and Geofencing

Hexnode equips your organization with location tracking policies to track and monitor your managed devices. This helps you locate your stolen or lost device. You can also set up a geofence and push differing policies when inside and outside the geofence.

Hexnode Messenger

Hexnode Incorporates its own messaging app – Hexnode Messenger – on Android, iOS and Windows 10 devices. It lets you broadcast messages to your user devices. With it, you can send one-way messages to target user devices and help in remote troubleshooting.

Management of Mobile Devices

Hexnode lets you manage and control all your enterprise endpoints from one centralized location.

Application Management

Hexnode lets your enterprise deploy apps to your managed devices with no user intervention. You can add or remove apps from the device and push policies to mandate

the installation of store or enterprise apps for Android, iOS, macOS and Windows devices. You can blacklist harmful and unproductive apps and whitelist work apps for Android, iOS, macOS and Windows. Also, you can push App Catalogs for Android, iOS and macOS devices and more, all from a centralized console.

File Management

Hexnode UEM enables businesses to manage and send files with its Mobile Content Management solution, including documents, applications, music and videos, to enrolled devices. You can also specify where the file can be stored. These files are silently downloaded from the server and can also be deleted remotely from the Hexnode portal.

Web Content Filtering

Hexnode enables you to push web content filtering policies to your managed endpoints and block access to unwanted websites. This keeps the corporate data in your devices safe from fraudulent sites.

Configure Wi-Fi and VPN

Corporate devices hogging open Wi-Fi networks are liable to cause disasters of biblical proportions. It would be best if you avoid them at all costs. Hexnode lets you prevent endpoints from connecting to unprotected networks. It also equips your organization with the ability to set up and configure Wi-Fi for Android, iOS, macOS, Windows and tvOS devices. This enables your endpoints to access the network without requiring a password for authentication. You can also configure VPN for Android, iOS and macOS, thereby providing a secure connection for your managed devices.

Configure Email and ExchangeActive Sync

Hexnode enables you to configure Email policies for Android, iOS, macOS and Windows devices. This reduces the number of steps required from the user-end and automates the configuration process. It is also possible to configure ExchangeActive Sync policies for Android, iOS, macOS and Windows and sync your user's email, contacts, calendar and notes that are stored in their Active Directory account to your enterprises' managed devices.

Enterprise Security Management

Remote Monitoring and Management software enables you to identify, track and neutralize potential security breaches before they happen.

Lost mode and Wipe device Actions

Stolen or misplaced devices can cause migraines in your IT department. Using Hexnode,

you can remotely push wipe actions or enable lost mode for your managed devices and protect the corporate data in them from falling into the wrong hands.

Enforce Password Policies

When it comes to corporate data protection, passwords are the first line of defense for your corporate endpoints. With Hexnode, you can enforce strong password policies on your enrolled devices and set up restrictions on password complexity, history, age, failed attempts and auto-lock time.

Device Encryption Policies

With Hexnode, you can configure and push device encryption policies, including FileVault and BitLocker for your Windows and macOS devices in bulk. This secures your data if an attacker tries to steal your hard drive and access it from another computer.

Work Profile/Business Container

Hexnode enables you to configure Work Profile for your Android Enterprise devices and Business Container for your managed Apple devices. This allows you to containerize and secure your corporate data from your personal data.

Seamless Onboarding and Integration

Import user information from directory services like Microsoft Active Directory and Azure AD, to enroll and assign devices to these users.

Zero-touch Deployment

With Hexnode UEM, you can streamline the enrollment of corporate devices to your portal. This is made possible by our integration with Android Zero-Touch, Apple Business Manager, Apple School Manager and Samsung's Knox Mobile Enrollment services.

Directory integrations

Hexnode's integration with directory services like Microsoft Active Directory, Azure AD, G Suite and Okta lets you sync user data and use directory credentials to simplify the enrollment process.

Zendesk integration

Hexnode provides easy ticket management solutions for your business with the help of Zendesk integration. With Zendesk Support, queries in the form of Help Center requests, emails, chats and messages are set to automatically create support tickets, that are then tracked, prioritized and resolved.

Automated Software Updates and Patches

Hexnode lets you remotely configure software updates and install the latest patches to your enterprise devices.

Configure and push OS Updates

Running an outdated OS can bring in many security issues for your enterprise. Also, for some companies, you need time to adapt your services to the updated device. With Hexnode, it is possible to enforce OS updates for Android and macOS devices and also delay software updates.

Push App configurations and Kernel extensions

Using Hexnode, it is possible to deploy app configurations for Android and iOS devices to suit the needs of your organization. You can also silently install kernel extensions for your macOS devices.

Conclusion

With Remote Monitoring and Management and its suite of tools and technologies, You can now achieve 24/7 monitoring of corporate endpoints. You can continuously track the status and health of enterprise endpoints and immediately identify and resolve discrepancies before they arrive.
Utilizing Hexnode's Unified Endpoint Management solution, you can implement advanced device management strategies to secure your corporate devices, all from a centralized console.