Remote Monitoring and Management for SMBs

An all-inclusive guide for your business

WHITE PAPER

hexnode

TABLE OF CONTENTS

Introduction

Remote monitoring and management (RMM) refers to the process of proactively monitoring company endpoints, networks, and software, by means of locally installed agents.

It enables IT to remotely monitor and maintain IT infrastructure from a remote centralized console.

Monitoring is a key part of any solid security strategy. However, manually monitoring all of your IT infrastructure, such as servers, desktops, laptops, and software, using traditional systems can slow your IT team down significantly. This is where Remote Monitoring and Management (RMM) software comes in. An RMM software combines two key activities – remote monitoring and remote management.

Remote monitoring involves observing critical IT metrics, and proactively identifying and resolving any potential failures within the network. Remote Management lets IT remotely control and administer enterprise operations from a centralized location.

Together, Remote Monitoring and Management software enables IT teams to continously monitor and perform remedial operations on IT infrastructure.

1

A brief history of Remote Monitoring and Management

Remote Monitoring and Management (RMM) systems were first developed around the late 90s, when organizations needed a more cost-efficient and less time-consuming method to provide continuous support and maintenance for their IT infrastructure.

Before the arrival of Remote Monitoring and Management (RMM) systems, organizations relied on the old on-site model of IT support, where IT technicians would go to the physical location at which the servers and endpoints were housed, and perform troubleshooting and repairs entirely on-premise.

This approach was also called the **break-fix model**, where issues are resolved only once they have arisen.

However, this approach proved to be highly time-consuming and inefficient, and organizations started looking for an alternative approach to support and maintain their IT infrastructure.

BREAKING OUT OF THE BREAK-FIX CYCLE

The issue with the break-fix model lies in IT teams having to wait for a fatal failure to emerge, which they can then address and resolve.

This often leads to last-minute solutions and temporary fixes, while a lot of time is wasted with the system being down.

> ***" It becomes difficult for businesses to ascertain the cost of IT support, as the services and expenses borne by the company is dependent on the number of times an issue arises within the network. "***

Drawbacks within the break-fix model of IT services

Let's take a look at why the break-fix model was considered inefficient for IT support.

Absence of network monitoring processes: With the complete absence of any network monitoring activities, organizations cannot determine points of weakness within the system. Hence, it becomes impossible to develop and enhance your IT infrastructure.

Budget uncertainty: With no sure way to ascertain when or how system issues may occur, organizations cannot determine projected costs for IT support. Hence, it becomes difficult to prepare their financial plans and establish goals.

Longer system downtime: With system issues being resolved only after they have occurred, system downtime is extended by a considerable amount. This, in turn directly affects business productivity and diminishes overall returns.

Zero visibility into threats: Organizations have zero visibility on potential threats and vulnerabilities. With no monitoring activities being performed within the network, minor issues that go unchecked may generate significant issues in the future, leading to chances of data breaches and attacks.

Ultimately, the break-fix model functions on the principle of reactive monitoring, which is an outdated approach. The current IT landscape does not offer the luxury of waiting for a system or server to go offline before beginning to fix it.

> ***" Much preferable is a system where IT can proactively monitor and maintain servers and endpoints, detect issues and resolve them before they even occur. "***

Remote Monitoring and Management (RMM) achieves this by operating on the principle of proactive management and providing IT with data on network status and health with early warnings when system quality is deteriorating.

THE HASSLE WITH LEGACY RMM SYSTEMS

The very first proactive IT support and services solution introduced by enterprises used the **Simple Network Management Protocol (SNMP)** to track essential health and status metrics on network endpoints and perform the required modifications.

However, they required a lot of up-front infrastructure and were extremely complicated to install and operate. As a result, only large enterprises could afford and effectively make use of these remote monitoring solutions.

Small and Medium Businesses (SMBs) often found themselves balancing a limited budget while ensuring they have the proper tools to monitor and manage their servers and endpoints. However, protocols in connectivity establishment and reduced overhead of maintaining connections have made RMM affordable and scalable over the past decade. As a result, SMBs can now leverage RMM technology to provide remote support.

2

The role of RMM in IT asset management

IT asset management plays a vital role in maintaining and monitoring your corporate infrastructure.

It ensures that your organization maintains a detailed inventory of all IT assets along with their current quality and health data.

Introducing a strong RMM solution to assist with IT asset management enables organizations to extend their existing capabilities by presenting a suite of advanced functionalities, including hardware and software inventory management, software license management, real-time monitoring alerting and reporting, remote network access, patch management, and more. This, in turn enables organizations to prepare for systematic asset expansion and retirement.

HOW AN RMM SOFTWARE WORKS

An RMM software helps businesses identify and resolve any problems within the company network. It works by installing an '**agent**' application on devices the client uses, including laptops, desktop tablets, wearables, and mobile devices.

These agents are responsible for feeding information regarding device status and health, thereby enabling IT to receive real-time insights into the company network. Once every device has an agent installed, IT teams can set up alarms and notifications if specific health and status thresholds are crossed.

It also enables IT to control and monitor remote devices, manage patches and security updates, collect and organize usage data, generate reports, and automate system maintenance.

If an agent detects an issue on a client device, an alert is automatically generated and sent to the IT team, giving them the necessary information to fix the issue. In some cases, these alerts enable the IT team to detect and resolve issues even before the clients become aware of them.

INTEGRATING RMM INTO THE IT SYSTEMS ENVIRONMENT

When integrating Remote Monitoring and Management (RMM) software into your IT systems environment, performing the following assessments enable organizations to identify unanticipated challenges, find solutions and ultimately assist with the transition process.

Step 1 - Assess the level of capabilities provided by the RMM solution

Before integrating an RMM solution into your IT environment, you must perform a thorough evaluation to ensure the software meets all of your organization’s IT support and service requirements. Any lapse in meeting requirements must be immediately addressed and resolved.

Step 2 - Fine-tune the configurations to fit your organization's needs

The next step involves identifying and documenting the configurations necessary to connect the new technology to the existing system, and determining the processes for completing tasks using the new software.

Step 3 - Assemble an implementation plan to merge the software into your IT environment

The next step involves identifying and documenting the configurations necessary to connect the new technology to the existing system, and determining the processes for completing tasks using the new software.

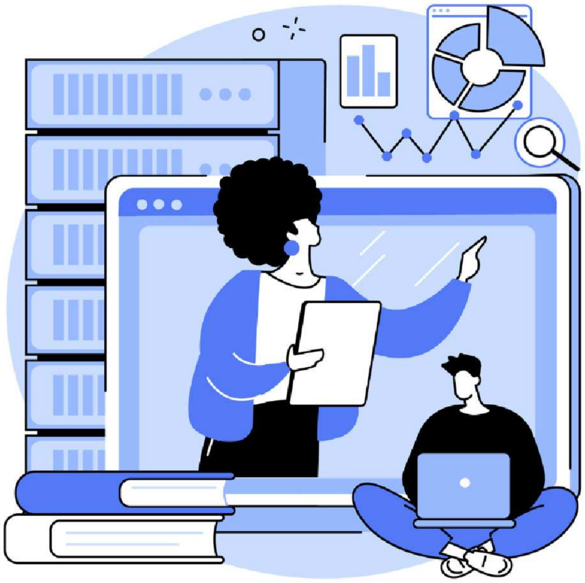
Step 4 - Integrate the software and perform periodic evaluations to ascertain it meets your goals

Once all the above processes have been completed, it's time to integrate the RMM software into your IT systems environment. There will always be challenges while introducing new technology into your existing environment. If any such problems arise, continue making iterations to the above processes until your organization completes a proper integration.

A final step for successfully introducing the new RMM technology is to **periodically evaluate its performance post-installation and determine how far it has helped you reach your organization's goals.**

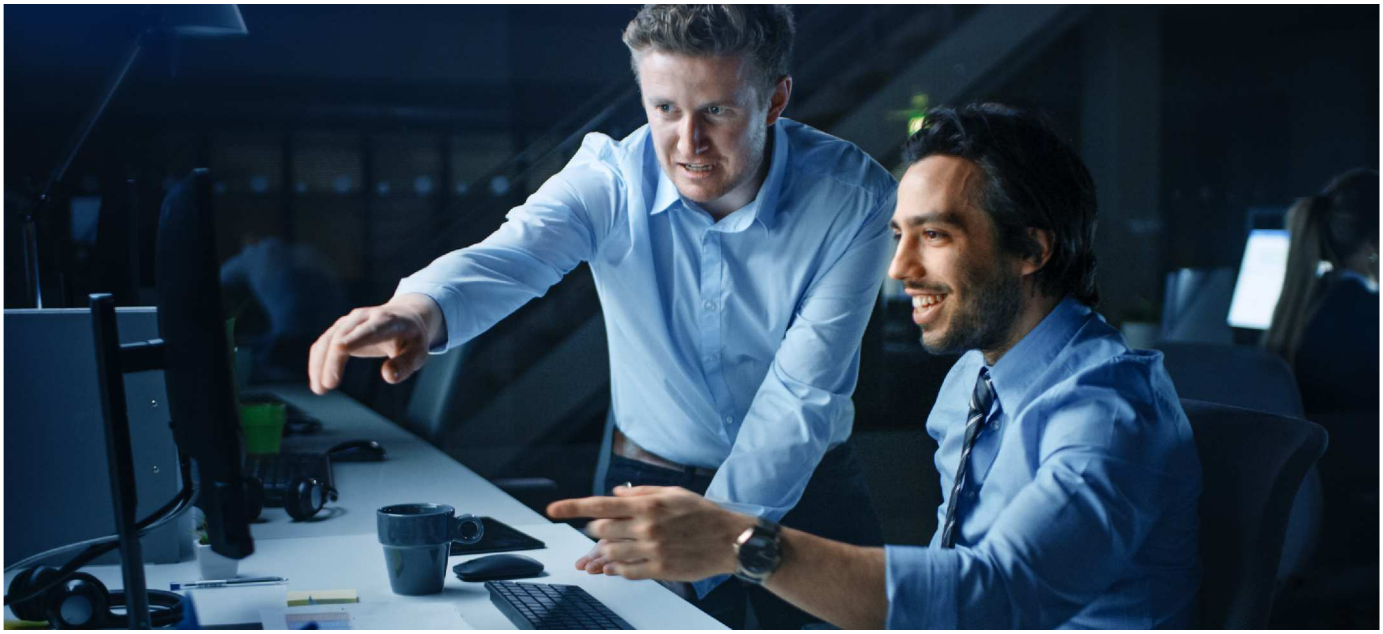
If you have not achieved a satisfactory result, **troubleshoot the processes, determine where your RMM solution is lacking, and resolve the irregularities.**

If you do not achieve a satisfactory outcome on multiple iterations, **evaluate further options for an RMM solution.**



RMM FOR SMBS – WHY IT'S NOT JUST FOR LARGE ENTERPRISES

With recent advancements in technology, and most of the IT infrastructure shifting from on-premise to the cloud, Remote Monitoring and Management (RMM) solutions have become feasible for SMBs and large businesses alike.



For small businesses, introducing an RMM solution into their IT environment enables them to cut costs on IT support and services and drastically reduce the time spent on the above processes.

What's more, with cybersecurity being a growing concern for all SMBs, implementing an RMM solution becomes crucial as it helps monitor and secure their network endpoints without requiring them to expend considerable manpower and resources on the same.

> ***" Today, any organization - be it SMBs or large businesses - can easily benefit from incorporating an RMM solution into its IT environment. "***

3

An overview of the core RMM functionalities

Although it is true that different RMM solutions cater to different business use cases and offer a variety of strengths and weaknesses, there do exist a collection of essential features and functionalities that every RMM solution must possess, regardless of the use cases it was designed for.

CORE FUNCTIONALITIES OF AN RMM SOLUTION

Here, we have compiled the list of the core RMM features and functionalities every RMM solution must have.

Migration and simplified deployment

Remote Monitoring and Management (RMM) solutions are designed to reduce the workload, time taken, and overall costs an IT team must endure.

However, if an RMM solution becomes too complicated to deploy and manage, it becomes detrimental to the entire purpose of introducing the RMM into your IT environment.

> ***" The RMM solution must offer effortless integration and deployment capabilities such that minimal time is taken to complete the initial process. "***

Usually, the process of deploying the RMM software involves installing an 'agent' app onto your network endpoints. These agent apps will then track and monitor the health and status of individual network endpoints, enable remote access to these endpoints, and provide even deeper management capabilities depending on the RMM solution used.

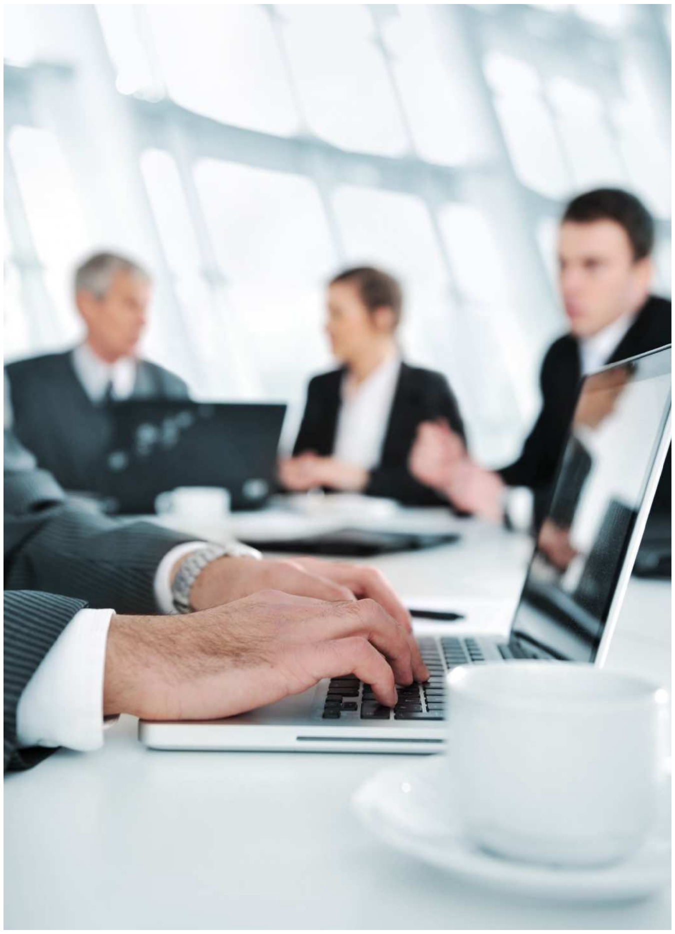
Hence, it is crucial to ensure that the deployment of these agent apps onto your network endpoints be as seamless and time-efficient as possible. A solid verification strategy is to check if your RMM solution supports any **zero-touch deployment** features and capabilities.

Remote access capabilities

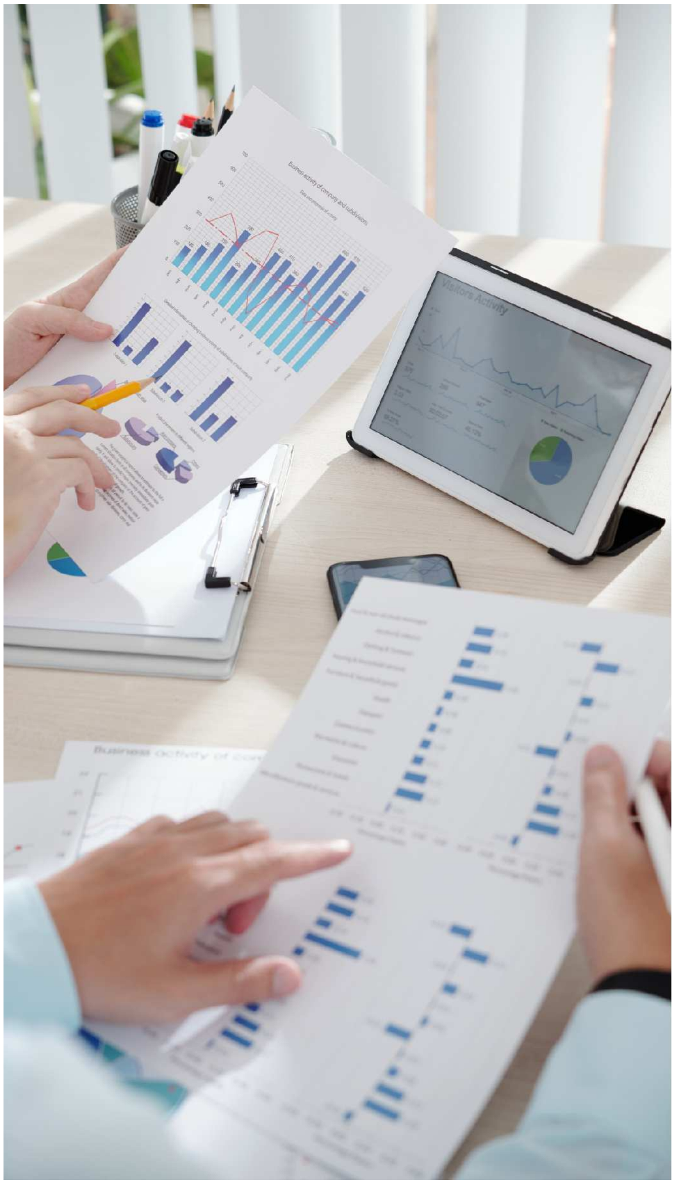
The ability to access a user's device remotely to troubleshoot and resolve issues is another essential functionality any RMM solution must possess.

Remote access refers to real-time monitoring and control tools that helps manage and access the device screen, execute admin actions and see crucial information including CPU data, running process, memory allocation and other details on the device. With a majority of the workforce going remote, the need for this functionality has become more crucial than ever.

> ***" Remote access can help the IT staff analyze the system, find and resolve issues critical to the device functioning, and thus reduce unexpected device breakdowns. "***



Multi-platform support



Your organization may use various devices and platforms for their day-to-day business activities, including desktops, laptops, smartphones, and tablets, all with different operating systems and security patches. Hence, it is crucial to ensure that your RMM solution is compatible with all the popular devices and platforms, including Windows, macOS, iOS, and Android.

Patch management

Patches are used to rectify vulnerabilities, improve software capabilities, and bring the software up to date. An RMM solution must have effective patch management capabilities for all platforms and operating systems and possess functionalities including determining the time at which updates should be installed, determining the status of patches and keeping a log of all patching actions performed by IT. This enables organizations to determine if their network endpoints are kept up to date, thereby preventing attackers from exploiting potential security vulnerabilities.

Auditing and reporting

An effective RMM solution should possess extensive reporting capabilities that enable organizations to track user and IT activities, monitor progress, and determine goals for their IT services and processes. A couple of standard reports that an RMM solution should maintain includes reports on endpoint status and health, RMM agent health, app and inventory audit, licensing information, patch management data, and more. What's more, your organization should be able to schedule and generate reports, export reports, and deliver reports via email, depending on their requirements.

These reports enable organizations to verify that their network and endpoints are healthy and enable them to compile data that helps them make better future decisions.

IT asset management

IT asset management is another core functionality every RMM solution must possess. A good IT asset management strategy enables IT to save time in logging and retrieving endpoint information including device attributes and status, location, installed apps, battery percentage, OS version, and more.

> ***" IT asset management involves the process of tracking, monitoring and managing the apps and devices in your network, by maintaining an inventory of the apps and devices you are managing and automatically updating this inventory whenever new apps or devices are added, or existing ones are removed. "***

In addition, changes made to the device can be automatically tracked and logged, thereby helping IT stay updated with their assets' health status.

Real-time monitoring and alerts

One of the core aspects of any RMM solution is the ability to monitor systems 24/7 and send alerts when issues surface within your network. The RMM solution you employ must be able to generate alerts on both overall system status and the status of individual applications and endpoints. What's more, IT should be able to configure custom alerts, tweak alert thresholds, and disable alerts such that unnecessary distractions do not burden them.

IT automation and scripting

Automating IT management tasks is another vital functionality that every RMM solution must possess. Most automation processes are performed using scripts. Hence, an RMM solution must support scripts written in many formats including MSI, Bash files, CMD files, and PowerShell. Routine tasks such as device and server maintenance, auto-remediation of issues, rebooting or shutting down devices can be automated with the help of scripts, thereby freeing up your IT team to perform more complex assignments and saving overall costs for your business.

Endpoint management

Endpoint management is an important functionality that every RMM solution must possess. It is an essential feature that helps complete the proactive IT support cycle of RMM services. For example, when an issue is identified on network endpoints via the RMM agent app, an alert is generated to the IT team. With the endpoint management functionality on RMM services, the IT team can remotely resolve or remediate the issue without any user intervention.

Hexnode equips organizations with the ability to perform a suite of endpoint management actions and functionalities on network endpoints.

RMM FOR PROACTIVE IT SUPPORT: WHAT SMBS NEED TO MONITOR

Remote Monitoring and Management tools provide organizations with a host of functionalities to oversee and manage network endpoints. However, as an SMB, it is essential to identify what data is crucial to monitor 24/7.

Here, we have compiled a list of the processes and information that SMBs must monitor.

Apps and system processes: Monitor essential applications and critical system processes and ensure they run correctly.

Endpoint status and health: Collect information on endpoint status and health, such as disk usage, CPU temperature, battery percentage, and more, to gain insight into the quality of your endpoints.

Device and app logs: Collect, maintain and view system and application log files and consolidate them in a central location, to determine the status, health, and action history on apps and endpoints and make better decisions with the information in hand.

Patch status: Determine if all endpoint, system and application updates have been installed. If not performed successfully, maintain logs on the reason for failure.

CPU memory and disk usage: Ensure that your network endpoints have adequate CPU memory and disk space to perform their jobs without encountering any hitches.

Network connectivity: Ensure that your network endpoints are online and connected to the corporate network. Monitor the security, health, and status of the company network.

Licensing status: Determine if all the required software licenses have been configured on your network endpoints and are valid.

Firewall status: Monitor firewall settings and ensure they are running correctly on your network endpoints.

Antivirus status: Ensure antivirus software is installed and running on your network endpoints.

Backup status: Determine whether your system has a backup in place and ensure that it is healthy and running successfully.

Firmware status: Check firmware versions and determine if all network endpoints are updated to the latest firmware.

Improper shutdown events: Ensure that improper shutdown events and problems are appropriately recorded and logged.

Step 1 - Review your IT environment and identify the key metrics that require continuous monitoring.

Step 2 - Adopt measures to perform 24/7 monitoring on critical processes.

Step 3 - Implement controls to notify admins and proactively resolve issues in the event of failures.

4

Evaluating an RMM solution for your business

Choosing the right RMM solution for your company can feel pretty overwhelming.

There are plenty of options available for businesses. However, it is important to identify your requirements.

This chapter goes over many of the key considerations that must be taken into account when selecting an RMM software for your business.

An excellent Remote Monitoring and Management (RMM)) solution helps businesses efficiently monitor endpoint metrics that are critical to business functioning and helps streamline the troubleshooting operations for IT.

When evaluating a new RRM solution for your business, there are certain things to consider before formulating your pros and cons list.

Various aspects, including pricing, features, ease of use, and your own business objectives, must be considered before committing to a particular solution.

KEY CONSIDERATIONS WHEN CHOOSING AN RMM SOLUTION

Here, we have compiled a list of the key considerations an organization must assess before choosing an RMM solution for their business.

Pricing

Pricing is a crucial aspect to consider when choosing an RMM solution for your business. The solution you choose must deliver a flexible and cost-effective pricing model. RMM solutions that offer a pay-as-you-go pricing are usually the best options for SMBs. Rather than paying upfront, companies can purchase licenses depending on how the business grows, and upgrade when necessary.

Scalability and flexibility

Scalability is essential to the growth of any small or medium business. As a result, the RMM solution you incorporate must also be equally scalable as your business. Flexible licensing enables SMBs to scale the solution according to their business growth. It also allows SMBs to try out the services and determine their value before making further advancements. Your RMM solution must possess the flexibility to expand both in features and supported users, thereby making it easier to grow your business.

Third-party integrations

When evaluating an RMM solution for your business, reviewing its integrations with third-party software and services can prove beneficial for your business.

Performing such a review enables you to determine a solution that works well with your already existing IT infrastructure.

For example, Hexnode offers enterprise integrations with many notable software and services, including Active Directory, Azure AD, and Google Workspace, thereby simplifying the process of migrating users and endpoints.

Continuous support

Implementing an RMM solution can be an intimidating process for SMBs. Without backing from a strong support team, IT teams can find it challenging to incorporate RMM functionalities into their environment. Hence, it is essential to determine the amount of support you will receive from your RMM vendor before choosing the right solution. Support functionalities include onboarding assistance, best practice guides, documentation and video tutorials, customer chat and call support, and more.

Centralized dashboard

Businesses often overlook the importance of a single centralized dashboard for RMM services. A centralized dashboard drastically reduces the time taken by IT teams to manage, monitor, identify and resolve issues on network endpoints. Hence, it is essential to review the dashboard's functionality of the RMM solution you consider. Check for functionalities, including customizable configurations on dashboards and a simplified view of the required information from the dashboard.

Automation capabilities

Automation enables SMBs to meet their IT needs while also eliminating the time required by technicians to perform routine tasks and optimizing the costs, thereby improving operational efficiency and technician productivity. It also helps bring consistency to IT support and services. When choosing an RMM solution for your business, ensuring that the platform's automation processes require minimal programming and effort can be highly beneficial for IT teams.

RMM AND ENDPOINT MANAGEMENT – HOW IT GOES HAND IN HAND

Endpoint management refers to the process of securing and managing corporate endpoints within a network. It helps companies ensure that endpoints are safe for corporate use, by assisting with deploying, securing, configuring and managing these devices.

Together with RMM, endpoint management forms an integral part of an all-inclusive software that ultimately helps IT provide a unified endpoint and network management solution for businesses.

Hexnode's Unified Endpoint Management (UEM) solution provides businesses such an all-inclusive suite of capabilities to achieve the complete lifecycle management of endpoints within the company network.

BEST PRACTICES FOR REMOTE MONITORING AND MANAGEMENT

Using RMM tools effectively can be challenging, especially for SMBs who haven't used RMM solutions in the past. Following are some guidelines that can help you ensure you are in line with all corporate procedures while making the best use of your RMM software.

Manage roles and access privileges

The first thing you need to do once you've incorporated an RMM into your IT environment is to add users and secure them. This includes assigning roles and access privileges, enforcing authentication with MFA and strong passwords, restricting admin access to only those who absolutely need it, reviewing user activities, and more.

Set goals and periodically assess their progress

Setting objectives and goals for your IT support and services practices and periodically tracking them enables you to receive a clear view of how well your RMM configurations have performed and determine if time and cost savings you have achieved match the bars set by your organization. This enables you to revise your policies and plans if the performance is unsatisfactory.

Avoid unnecessary alerts

For most organizations, especially SMBs, monitoring and managing every attribute for your endpoints and networks is not quite feasible. Attempting to do so will result in your IT team being overwhelmed with alerts. Rather, it is more viable to personalize and set up alerts according to your business requirements, only for critical issues, and disable alerts related to unnecessary metrics.

Start small and scale up

When onboarding an RMM solution for the first time, quite a few businesses (most notably SMBs) may find it difficult to fully utilize all the features and functionalities provided by the RMM, especially if the software proves to be complex. In such cases, instead of drowning within the technicalities of all its features and functionalities, it is more comfortable, to begin with, just the essential features and scale up as you learn more about how the solution works and how to take advantage of its features.

Conclusion

Remote Monitoring and Management (RMM) and its suite of tools and technologies eases the process of monitoring and controlling corporate infrastructure.

Businesses can continuously track the status and health of enterprise IT systems - such as servers, endpoints, and software - and immediately identify and resolve discrepancies before they arrive.

As we have seen, adopting an RMM solution for businesses can go a long way in easing up the burden on IT teams.

Learning and understanding the key features, benefits, and differences between the host of RMM software available, will help companies - especially SMBs - to choose the best solution for their requirements.

Hexnode's Unified Endpoint Management solution, equips businesses with advanced RMM capabilities to secure, monitor, and troubleshoot corporate endpoints, all from a remote centralized console.