N-ABLE™

Changing RMM Tools

How to know when your MSP has outgrown its RMM Tool

eBook

Table of Contents

Introduction

As an MSP business grows and develops, it's likely they are going to find that the tools they originally chose to support the business may not be enough for their current needs. No vendor wants to lose customers, and MSPs want to make sure they are using their existing tools to their full capacity. There are going to be times when their existing toolset can hold them back, and the MSPs serious about growth need to know how to identify when it's time for a change.

To help negotiate this crossroads, this eBook will look at some of the indicators—both the obvious and the not so obvious—that can signal a time for a change in Remote Monitoring and Management (RMM). And if the tool still fits? We've included a list of things MSPs should be doing to keep tabs on the performance of their RMM.

Signals that indicate it's time for a change

The "red flags" in this initial section may seem obvious to some, but they may not be for all. It is important as business leaders to be mindful of the signs that the tools or partnerships you leverage are helping grow your business.

Unable to scale with the demands of the business

If the business is struggling with managing and monitoring the number of devices it supports in their environments, then something isn't right. One of the primary signals that indicate change is needed is if the business is suffering major growing pains as they scale. Some examples of growing pains an MSP might encounter include slow onboarding of new customers due to manual agent deployments or a lack of quality automation in key parts of the process.

Low confidence can lead to lack of RMM usage and downtime

Another area of concern would be if techs are losing confidence in the data and alerts produced by monitoring cycles, which could happen for several reasons. For example, if alerts are stalled or misconfigured, this could result in them becoming background or white noise and therefore unattended. This reactive business model can have a major impact on incident remediation. Techs may be required to drive onsite to resolve problems, leading to a loss of time and productivity. As we shift more and more to increased efficiency within the MSP sector, this would be a practice best avoided.

Lack of confidence in monitoring results can lead to costly downtime.

Another all-too common sign of RMM failure is "patch mismanagement". If the staff is underutilizing the RMM to detect, deploy, and approve patches, it may be because it is not configured correctly, but equally it can be a sign that the RMM is insufficient. If techs start to experience "white noise" with patch alerts, it could lead to costly downtime if something is missed.

Prioritize monitoring patch statuses efficiently and effectively

The staff is feeling the pressure and speaking up

If the staff feels like they've lost trust in the RMM and its ability to deliver, it's a strong indicator that it might be time for a change and to look at something fresh. The challenge in bigger organizations is that it can be difficult for people at the manager level or above to have the functional and performative insight their techs do. So, what are the types of things that techs might be saying that would indicate to leaders that there's a problem that needs investigating?

If techs are coming to management and saying, "We finally finished that new customer roll out, but it was a lot of work," what they probably mean is there was a lot of **manual work.**

The onboarding process is a critical part of the customer experience. Although it's not a big revenue generator, it needs to be efficient. If project timelines are extended to onboard a new customer or if staff are having to manually deploy agents, this could be a sign that the RMM is not working hard enough for the business. It's time to take a step back and look for improvements you can make to the process.

If a tech says, "we finally got all the alerts cleaned up—**what a mess!**" , that could be a sign that the alerts are being neglected due to "white noise".

If a tech is having to wade through "white noise", this puts them at risk of working reactively to a large, variable list of alerts versus using the RMM tool to prioritize them. This problem can arise due to something within the customer's network environment, but it can also be a resourcing issue—their RMM just isn't capable of adding another hundred or thousand devices while running new discoveries at the same time across multiple devices. Additionally, if management is told that the alerts are not there on half of the devices, that too is a red flag.

It is important that business leaders regularly ask questions like "is it time to start fresh on my existing solution?" or "Is there something better out there to meet our needs?" Ripping out and replacing something so critical to the operation of the business is no small ask. It's worth making a list of the key issues the business is facing and the new criteria by which the team needs to evaluate performance. This will not only aide in evaluating new vendors, but it can also help highlight clear talking points with the current vendor.

Looking to re-onboard is a good first step, as it can be cheaper, easier, and less of a burden (including requiring less training) than tackling other functional issues. This is especially true if the existing RMM is fundamentally solid and ticks all the boxes for what is needed. But that doesn't mean it's the only answer. It might require a deeper dive into some less obvious signs that it is time for a change.

Have I outgrown my RMM? The less obvious red flags

Now that we covered the most obvious signs that an MSP business might have outgrown its RMM, it is time to look at the less obvious red flags that could be lurking.

Is your customer onboarding painfully manual?

To start, let's go back to onboarding customers. When I was an MSP, probably similarly to most MSPs, I had some 27 things on my onboarding checklist. So, when a new customer came in, I'd work my way through that list to bring them onboard and into our RMM. In the past, a lot of manual effort was required to do this, but with enhancements to the automation capabilities of RMM platforms, this doesn't need to be a slow or manual process any longer.

If the business can't (or is struggling to) set up automations to enable the discovery of new devices, see what type of devices there are and then automatically put them into a patch or a monitoring profile. This is a good example of the business taking full advantage of the RMM's capabilities and quite possibly that it has outgrown them.

Related to this is another key requirement that, if not met, should raise a red flag. Talking to customers to establish what their business-critical systems are is crucial. Lacking the ability to tailor monitoring to specifically target and support those business-critical systems to help meet SLAs is a big problem. If this is not something you are able to customize inside your RMM, you may not have the right solution to meet your customers' needs.

The RMM stops being the go-to platform

For an MSP, an RMM product should be one of the core platforms used alongside PSA and backup products.

If the business is not looking at the RMM as the go-to platform for monitoring, patch, and remediation, then that's a major red flag.

Techs should not be receiving alerts and immediately thinking "let's remote in", rather than trusting the RMM platform. If staff would rather spend a bunch of time poking around in a user's machine, this could be a clear indicator that they've lost trust in the RMM and, as a result, are not using it to its full potential. If they're trusting their own IT skills against having faith in the functionality of the RMM to run things like self-healing or automatically remediate issues, then management needs to understand why.

If trust in an RMM is lost, MSPs may pick up another tool to do what the RMM was meant for.

There may be a justified reason for bringing in additional tools, like if the environment needs a specialized monitoring package that common RMM's don't provide. In some cases, the reality is that the care and attention that goes into keeping an RMM's monitoring capabilities working effectively has not happened for some time. In this instance, an MSP might bring in a new tool that overlaps with capabilities the RMM already has, leading to redundancies, additional costs, and loss of efficiencies.

Unwilling to provide RMM access to customers for visibility

Having lost faith in the RMM product can also manifest itself in another way: the business is unwilling to provide RMM access or reports to customers for visibility. If the business is not happy putting the RMM in front of clients, then this could be yet another soft sign that it's time for change.

Food for thought: If an MSP doesn't trust giving customers access to see the work done or give clients access to remotely connect to their own devices, is this because of a lack of trust in its role-based permissions?

If, while reading this eBook, you are mentally checking several or all of these boxes, then maybe it's time to have a serious conversation with the RMM vendor and the staff.

With a good grasp of obvious and less-obvious red flags that the RMM is not meeting the needs of the business, the next section will cover how to review the health of the RMM on a routine basis to avoid leaving things to the last minute. The effects of not staying on top of RMM health can lead to damaging the relationship with clients, the vendor, and forcing the business into an unnecessary change.

Outgrowing your RMM health check list

This section will cover several areas that can be used to get a better understanding of the current health of your RMM. It can help decide when it's the right time to upgrade to a new solution and a vendor.

RMM Product Usage Assessment

Monitor how the business is using the RMM, particularly in common use cases like onboarding new customers, proactively monitoring environments, remediation alerts, and patch management. Make sure to find out whether the techs are confident in the results they are getting in these areas and happy with the processes they've created. Doing this regularly will present an opportunity to spot problems early and go back to the vendor for help.

RMM Platform Health Check

This is the next step if there are product usage issues, but it is also worth periodically checking as a standalone issue. A full health check will help identify areas for improvement to align with best practices and operational efficiency within the platform.

This is where the need for the vendor's support staff comes in. Someone from a vendor's organization should be able and willing to work with the business to make sure the product is being used correctly, or at least to its optimum capacity for the business's particular needs.

I know that across our partner base there are people using our products in a simple way and others using them in an advanced way. Optimum usage is dependent on the individual MSP, but your vendor can still help ensure you're using all the features and functions you need and that you have properly integrated the product into the different parts of your business.

Scale and Standardization

Often, MSPs and IT departments are faced with rapid growth. This is a critical time when an RMM is a key business system. If there are signs that the ability to scale or automate onboarding, configuration, and standardization of settings and polices is not possible with the current RMM, it might mean it's time for a change.

Additionally, considering the growth needs of the business, it might be worth a deep dive on how the hierarchy and structure of the RMM platform helps drive and manage multiple levels of automation. Is it easy to create filters and take actions? Is it easy to group, and sub-group, then leverage those filters and groups anywhere in the solution?

These are smaller issues that can go unnoticed but evaluating them periodically against the goals and growth objectives of the business can help predict future growing pains.

How much is in the box?

Consolidation can have a double edge. On one side, having a single solution that attempts to do everything can result in less depth and less control; on the other hand, it can also mean management, training, costs, and upkeep of multiple solutions.

When it comes to critical workloads such as patching, automation, security, network discovery, and even asset management, the RMM should not require multiple products/vendors to achieve a solution. For example, patching of third-party applications, as well as install and removal of wanted/unwanted applications, should be "in the box" functionality and not require additional tools or products.

Ask yourself: "Is the RMM vendor prioritizing 'in the box' or 'out of box' on key workloads?"

Staff Validation

It can be a difficult thing to gather direct and unfiltered feedback from staff. There can be situations where feedback seems rooted in "today's problem" or "we have heard this all before." A critical part of maintaining a successful RMM platform is ensuring that the staff are happy and engaged.

To regularly temperature check staff, I suggest holding staff-led feedback sessions. Let the staff lead the discussion; let them set the priority on what is first in line for a change or where help can have the biggest impact. This can go a long way in not only having a healthier RMM, but more satisfied employees.

Peer Validation

Finally, use the communities that are out there to talk to other like-minded businesses. Having insight from other people can potentially help you understand and see the true value of your RMM, as well as helping to recognize places where it might be underutilized in your company.

Ultimately, it's on the leaders of the business to help drive and identify areas where more support is needed, but an MSP must be ready and capable of providing the support they need. The MSP should be able to say, "Here's where you are today. Here's where you're doing well and here's some of the areas where we would recommend you make some changes." The MSP cannot tell the business how to work with their customers, but they can make recommendations based upon what others are doing and knowing how their products work.

A vendor who is not willing to help to this extent might be a sign that the partnership has been outgrown, even if the technology requirements are there.

Conclusion

Given how critical an RMM can be for a MSP or an IT department, it should be clear that validating how it is performing against the business's changing requirements is a must. Having spent many years in the industry and well over 10,000 hours engaging with MSP's and IT professionals, it can be difficult to hear the challenges faced and the impacts of not identifying and acting on the signals that indicate a change is needed.

Not acting on migration needs regardless of if they are technical, partnership-related, or both could have serious and long-lasting effects on the business. Ideally, after reading this, the first actions should be to start watching for the signals, listening to the staff, and planning your RMM health checks.

About the Author

Chris Massey,

Senior Manager of Partner Growth, N-able

Chris has over 13 years' experience in leading service delivery, technical operations, product, and marketing teams for an Enterprise MSP. He helped grow a service provider from 25 to 280 employees over a decade and was a key part of several organic growth and M&A activities for the service provider. Chris is focused on working with partners to overcome common challenges they experience with the MSP.

N-able

N-able fuels IT services providers with powerful software solutions to monitor, manage, and secure their customers' systems, data, and networks. Built on a scalable platform, we offer secure infrastructure and tools to simplify complex ecosystems, as well as resources to navigate evolving IT needs. We help partners excel at every stage of growth, protect their customers, and expand their offerings with an ever-increasing, flexible portfolio of integrations from leading technology providers. n-able.com