TeamViewer
Remote Management

WHITE PAPER

4 Keys to Managing IT Remotely

Contents

Introduction:
Advantages of Remote IT Management

IT is most valuable when it maximizes the effectiveness, security, and efficiency of the IT infrastructure, keeping organizations as productive as possible. Meeting that goal requires replacing the traditional reactive break/fix paradigm with a proactive approach designed to keep systems running instead of waiting for them to break.

This paradigm shift from reactive to proactive is underscored by the still-growing number of former IT contractors that have become managed service providers (MSP). In just six years, from 2018 to 2023, the global market growth of managed service providers is expected to rise from $173.4 billion USD to $296.38 billion.[1] Their goal is to identify potential problems and address them before they cause unplanned downtime and costly repairs.

When every deployment, update, or repair requires an in-person service call, it's difficult to take a proactive approach to IT because you are always reacting to ad hoc incidents. Businesses must decide for themselves when their IT infrastructure has outgrown reliance on 100 percent in-person service. Once IT serves a network with five or more devices and there are some people working remotely, it's time to compare your current IT support costs — including the costs of unplanned downtime — with the projected costs of proactive remote IT management.

The advantages of a well-designed remote IT management solution become indispensable once it enables MSPs and IT departments to do *all* of the following remotely:

- Run and maintain IT infrastructure to significantly reduce the average ticket response time
- Perform maintenance tasks during off hours to avoid interrupting employees
- Be proactive instead of reactive by keeping software current and safe from cyberattacks, with endpoints protected and data backed up
- Gain real-time insights into IT infrastructure and share them with business stakeholders to help evaluate current conditions, make timely decisions, and project future needs
- Boost operational efficiency and reduce costs by monitoring devices and addressing potential problems before they become major issues

With the growing popularity of remote IT management, the number of IT services that can be provided remotely has also expanded to include network monitoring, device monitoring, patching, web monitoring, endpoint security, endpoint backup, and more. These services are bundled and offered as remote monitoring and management (RMM) solutions.

According to Smarter MSP,[2] an experienced MSP product marketing manager indicated RMM solutions enabled these three key benefits for MSPs:

1. Increase efficiencies by having a complete view of managed assets and delivering services quickly and seamlessly.
2. Ensure maximum uptime by monitoring networks and devices, enabling them to act quickly on alerts of potential problems before they escalate.
3. Reduce expenses by eliminating the need for travel every time support is needed.

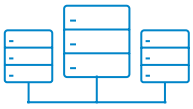
These benefits apply to internal IT departments as much as they do for MSPs, especially with remote workforces.

Many RMM solutions can be tailored to IT requirements, so you only get the options and services your organization needs. In this white paper, we will cover the four keys to managing IT remotely, along with the available options to consider for your RMM solution.

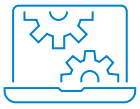
Four Keys to Managing IT Remotely

1 Know What You Want IT to Monitor and Manage Remotely

Not all RMM solutions are alike. Most RMM solutions help you monitor and manage some or all of the following:



Data Centers

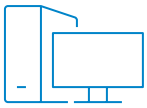


Operating Systems

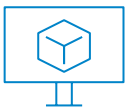
Servers

Applications

Websites



Endpoints



Virtual Machines

Peripheral Devices

2 Have the Right Tools for the Job

Prioritize. Create a list of challenges and problems your organization is facing. Which issues require immediate attention? Once you define the top challenges, you can prioritize which tools are absolutely essential. From there, decide which tools you may need in the near future and which ones are irrelevant.

Here's an overview of available RMM tools and services. Which ones are business-critical for you?

24/7 Real-Time Network and Device Monitoring

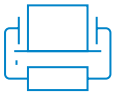
Monitor servers and endpoint devices 24/7 and get real-time alerts of potential problems, so you can address issues before they escalate.

Asset Management

With full visibility from an asset management console, you can see, monitor, and manage every device in your IT infrastructure from one screen.

Patch Management

Timely and automated mass patching of operating systems and third-party software protects against cyberattacks that exploit software vulnerabilities.



Network Device Management

Monitor and manage the availability of network peripheral devices, such as printers, routers, firewalls, switches, USBs, and more.

Endpoint Protection

Centralized and automated anti-malware protection for desktops, laptops, tablets, and smartphones significantly reduces the risk of viruses, ransomware, spyware, and more.

Backup

Managing backups remotely ensures that this critical element of every business recovery plan is executed thoroughly and on schedule.

Website Monitoring

Monitor your website from multiple locations and get alerts if your site is loading too slowly, not accessible, or has functional problems (e.g., e-commerce checkout errors or customer login failures).

Mobile App

Enables IT technicians to operate RMM from their Android or iOS mobile device, so issues can be identified and addressed from anywhere, 24/7.

Reporting

Generate detailed reports on server uptime, malware detections, issue resolution times, and more. Get custom automated reports for the KPIs you specify.

Auditing

Keep track of third-party software license compliance, so you always know how many licenses for each software application are in use as well as how many are still available.

Network Discovery

See when new devices have been added to the network to ensure proper setup and remote management.

Mobile Device Management

Along with desktops and laptops, monitor and manage smartphones and tablets.

Integrated Ticketing

Organize and manage all support tickets in your RMM, whether submitted by phone, email, or an online help desk form.

Application Programming Interface (API)

Enables you to read the data collected in and reported by the RMM solution in third-party software as well, so it can be shared with units that don't have access to the RMM.

Software Deployment

Deploy new software to tens, hundreds, or thousands of devices in the background without affecting employee device usage.

Scripting & Automation

Script routine tasks: schedule to run repeat processes automatically (e.g., create system restore points or delete temporary files at specified frequencies).

Professional Services Automation (PSA)

Professional Service Automation can work with or be part of the RMM solution to help manage MSP businesses by integrating ticketing, providing business insights, scheduling technician time, and streamlining billing.

Work with RMM vendors that offer all the tools you need and allow you to customize your solution, so you don't end up paying for unnecessary tools and services.

Manage Securely

According to Statista, the average cost of a cyberattack for European or North American businesses with 50 employees or fewer in 2020 was $24,000 USD; $133,000 USD for those with 250-999 employees; and $504,000 for those with over 1,000 employees.[3]

Given the high costs businesses incur because of data loss, malware, zero-day attacks, phishing, ransomware, and more, having a secure RMM solution with tools to keep your network and devices secure is essential.

While your RMM makes it easier to manage the security of your IT infrastructure, it's also important to consider the security of the RMM itself, because an RMM solution connects with every part of your infrastructure. Some RMM solutions may also connect with third-party software. If there are vulnerabilities in those connections, your company could be at risk. One security researcher published information about such a vulnerability in a popular RMM tool in 2017. Two years later, an MSP that hadn't patched the vulnerability saw their entire client base crippled by it.[4]

Three RMM tools — patch management, backup, and endpoint protection — handle common IT security challenges. Integrated RMM solutions enable you to perform security-related tasks without having to toggle between applications. RMM also gives you at-a-glance insights about your devices, with details such as:

- Which devices require patching for operating systems and third-party applications
- Whether all device backups were successful
- The current status of endpoint device protection

Endpoint protection notifies you if a device has been the target of an attack, so counter measures can be taken immediately *and* remotely. With RMM, your IT technicians don't have to handle device issues in person in order to take action. They can resolve urgent issues anywhere, from wherever they are.

To ensure a third-party or intermediary can't decipher transmissions to or from your RMM, every remote session you have with your servers and endpoint devices must be protected by end-to-end encryption. Other critical RMM security features include:

- Assurance from potential RMM partners that they patch vulnerabilities upon awareness
- Administrative ability to permanently remove and deny access to former employees
- Protection against key logger and brute-force attacks

With the right RMM solution, the platform itself should be secure with integrated RMM tools that help manage your IT security.

Simplify Your Tech Stack

Whether you're an internal IT manager or an MSP operator, efficiency has to be a top priority. At the speed of business today, inefficiency leads to chaos, security risks, and bad customer experiences, just to name a few.

You can probably find a different vendor for each of the tools you use to manage IT remotely, but one of the biggest benefits an RMM provides is the ability to consolidate your tech stack by getting all the tools from one provider. Having a centralized RMM platform with all your remote management tools offers three main advantages:

1. **Increased Efficiency**

   Monitor and manage every device from one screen. That means your IT technicians don't have to switch back and forth between platforms every time a new device or user is added to the system and every time they need to access a different RMM tool.

2. **Total Peace of Mind**

   Eliminate concerns about potential solution incompatibilities since all tools and services are integrated into one platform.

3. **All-in-One Convenience**

   Having one vendor to work with means one sales person, one support number and email address, and one invoice to pay. Having two or more vendors for your remote management tools adds complexity and more administrative work for all stakeholders and departments involved.

RMM goes hand in hand with remote access and support. How? When issues are identified with RMM, you can use remote access to connect to the device and resolve problems immediately — all from one integrated platform.

You can streamline your IT tech stack with RMM and remote support, available in the same integrated platform from TeamViewer.

The TeamViewer RMM Solution

TeamViewer Remote Management is a robust solution for remote IT management that offers Remote Device Monitoring, Network Device Monitoring, Asset Management, Patch Management, Endpoint Protection, Backup, and Web Monitoring. While TeamViewer Remote Management is available as a standalone solution, it also works seamlessly with TeamViewer Remote Access and Support, so your remote management tools are always reliable, fast, and secure. For users of TeamViewer Remote Access and Support, TeamViewer Remote Management is a convenient, integrated extension.

Conclusion

Proactive remote IT management is much more efficient than the old break/fix approach that required technicians and devices to be in the same place. The range of functions and devices that can be managed remotely continues to grow. RMM has made remote IT management even more efficient by bundling tailored sets of tools into one platform, allowing organizations to consolidate their tech stacks and perform all remote IT management functions from one platform.

When TeamViewer RMM is paired with TeamViewer Remote Access and Support, IT organizations and MSPs work faster, more securely, and more productively than ever before. Using these four keys to managing IT remotely, you can unlock the right RMM solution for your company.

Next Step

Want to evaluate TeamViewer RMM for your company? Test all the features and services with a free 14-day trial.

Request Free Trial

No obligation, no credit card required.

TeamViewer

Resources

Learn more about TeamViewer RMM

Request a free demo of TeamViewer RMM

References

1. Impact (2020, June): Why the Break/Fix Model for IT Services Is Dying. Retrieved from https://www.impactmybiz.com/blog/why-the-break-fix-model-for-it-services-is-dying/

2. smartermsp.com (2020, July): Ask an MSP Expert: How can an RMM tool help my MSP business? Retrieved from https://smartermsp.com/ask-an-msp-expert-how-can-an-rmm-tool-help-my-msp-business/

3. Statista (2020, November): Average cost of cyberattack to European and North American firms 2020, by size. Retrieved from https://www.statista.com/statistics/1008112/european-north-american-firms-cyberattack-cost/

4. securityboulevard.com (2019, February): Ransomware attack on MSPs exploits popular PSA/RMM Tool. Retrieved from https://securityboulevard.com/2019/02/ransomware-attack-on-msps-exploits-popular-psa-rmm-tool/

About TeamViewer

As a leading global remote connectivity platform, TeamViewer empowers users to connect anyone, anything, anywhere, anytime. The company offers secure remote access, support, control, and collaboration capabilities for online endpoints of any kind and supports businesses of all sizes to tap into their full digital potential. TeamViewer has been activated on approximately 2.5 billion devices, up to 45 million devices are online at the same time.

Founded in 2005 in Göppingen, Germany, TeamViewer is a publicly held company listed on the Frankfurt Stock Exchange, employing about 1,350 people in offices across Europe, the US, and Asia Pacific.

Stay Connected

www.teamviewer.com

TVRM-WP-EN-EMEA-012021-1