

TOSHIBA

Whitepaper

Manage your IT and protect your business with RMM



**TOGETHER
INFORMATION**

Today's organisations must rely on technology to gain an edge. However, maintaining, monitoring and securing such technology can be time-consuming and expensive. Remote Monitoring and Management (RMM) offers a great solution for small and medium businesses (SMBs). Freeing up in-demand IT teams to focus on value-added activities - boosting productivity, improving security and positively impacting the bottom-line.

With RMM, unusual behaviour and possible malware are automatically flagged for review, making your cybersecurity much more robust. Which is essential at a time when data breaches are on the rise. No SMB can afford the reputational, trust and financial damage that comes with a data breach.

RMM comes with additional benefits in increasing equipment lifespan, reducing downtime, scheduling maintenance and ensuring network stability.

Discover more about how RMM can help you. In this whitepaper, you'll learn how RMM can help your business and how to choose the right solution.

The status of IT infrastructure management

Businesses today have a large amount of IT infrastructure to manage on a day-to-day basis, adding to the ever-increasing workload. Even virtualized infrastructure requires constant management to ensure smooth operations.

This is made all the more difficult if your technology is dispersed across multiple locations - if your workforce is remote, for example, or you have more than one office to maintain. Tracking IT assets spread across your offices can quickly turn into a nightmare. Especially if any equipment fails, requires maintenance or is compromised. Spending hours manually checking event logs for such incidents is also time-consuming for in-demand IT managers who could be better utilised elsewhere.



Remote Monitoring and Management

Remote Monitoring and Management (RMM), also known as network management or remote monitoring, offers a cost-effective way to reduce an in-house team's workload and focus efforts on other value-added activities.

By 2020, [60% of organisations](#) will have experienced a major service failure. Resulting in expensive downtime, a possible data breach, loss of goodwill and a damaged reputation. The consequences of a service failure or cybersecurity breach can take months, if not years, to repair, not to mention the financial implications involved.

The benefits of RMM

With RMM, a software footprint known as an 'agent' is installed on your server and/or workstations. These agents provide 24/7 monitoring of your machine health and status, constantly checking event logs for potential issues. This is fed back to a centralised expert team. Allowing for easy machine maintenance, ensuring they are always up-to-date. Issues are resolved quickly and managed proactively.

Some benefits of using a RMM solution are:

- **Helps SMBs with enterprise-level automation and monitoring.**
- **Helps detect issues before they cause downtime or critical system failure.**
- **Helps in the systematic management of clients' IT requirements.**
- **Helps ensure optimal network stability.**
- **Helps enhance the performance of clients' systems.**
- **Helps extend the lifespan of clients' systems and devices.**

The agent can identify incidents which are then raised as a ticket in a service management system. A key benefit of RMM is to identify and then fix the incident fast. As it is automated, this means not having to rely on manual intervention.

Applying patches to systems can be a daunting prospect - if you apply patches are there going to be unknown issues once they are applied? [Patching](#) can plug gaps in known software bugs and decrease the vulnerabilities these can cause.

Remote patching can relieve this burden by automatically applying updates once the patches are fully tested; so reducing the potential impact of applying untested patches. If there is a requirement to reboot these can be scheduled so as not to interfere with the working day.

RMM and small businesses

For SMBs, using an RMM agent can prove invaluable as it delivers enterprise-level automation and monitoring, but in an affordable and scalable manner.

Using RMM ensures that downtime is kept to a minimum, increasing productivity and improving the bottom-line. With proactive maintenance, device lifecycles are extended. Meanwhile, in-demand IT managers can focus on strategy and preventative measures, rather than break-fix issues and firefighting.

The features of a good RMM solution

Effective RMM solutions have a wide range of features that allows for better remote management of a network. As a minimum, you should look for a solution with:

1

Deployment and scalability

A good RMM tool can be easily deployed and will scale with your business. As you add more devices and premises, the RMM should be able to enrol more end-points with ease.

2

Remote access or screen sharing

Enabling technicians to remotely connect to systems at the click of a button without input from the end-user. Quick access allows for rapid response times and a better experience for customers.

3

Patch management

Patches are rolled-out automatically based on policy settings. The RMM tool should also automatically log a support ticket if any issues arise during installation, so nothing is left to chance.

4

Anti-malware and antivirus

[42% of SMBs](#) experienced a data breach or attack in the last 12 months. Central management of anti-malware and antivirus is essential to maintain reputation, customer trust and business operations. With RMM, an agent will quickly log a ticket if it detects a possible virus or other activities that aren't the norm, such as updates not loading correctly.

5

Remote software installation

The RMM will allow for the set-up of a script to install software across all of your devices, without having to manually connect to each one.

6

Hardware failure

When a server hard drive fails, you need a quick resolution before problems escalate and threaten business continuity. The RMM agent can constantly monitor all of your hardware to detect the potential of failures and automatically alert technicians.

7

Hardware and software auditing

Auditing hardware and software is much easier with RMM involved as it already has the part and serial numbers required for the audit. By running an auditing report through the RMM, you can easily see a list of all devices and their warranty status, the amount of software installed on your systems and much more.

8

Scheduled reboots

A RMM tool should allow you to schedule reboots outside of office hours, to prevent disruption to the working day. It does away with manual reboots and doesn't involve connecting a device to a system to reboot. Instead, devices will reboot automatically overnight, completely unattended and all controlled via a user-friendly RMM dashboard.

Concerns for IT Teams

For small companies, a failed patch roll-out is painful. For large organisations, it can cause as much impact as a cyber attack, stop thousands of people from working, and require substantial resources to fix.

If a small business does not have an IT expert available for their infrastructure, maintaining updates can cause potential risks to their business. Risks associated with outdated operating systems, that should not be on a network, can have far-reaching consequences.

An RMM agent can assist in discovering what operating systems are on the company network and how many there are. This way you are better informed of the current footprint of your network infrastructure.

RMM solutions help to address many challenges facing SMB leaders. A RMM system strengthens the protection and maintenance of business-critical IT infrastructure. It mitigates cybersecurity risks.

Businesses are powered by a wide range of devices and large numbers of devices can only be managed properly via a RMM. The more devices your business uses, the higher the risk of a data leak. RMM tools also alleviate the pressure on in-house teams, enabling them to work on more strategic and valuable tasks.

Nearly [2 million SMBs](#) lack the digital skills and knowledge needed to drive progress. A lack of basic digital skills in SMBs has led to five million working hours every week being lost through fixing every day IT issues such as computer crashes.

Preparing for the digital-first world

To prepare for an increasingly digital world, SMBs and their IT teams (if available) must be equipped with the best tools available. Using a RMM will transform your business' productivity, continuity and support.

RMM is essential for every IT-driven business. No matter your company size, it will benefit from using an RMM solution at some stage in its growth. Technology will underpin every market leader in the next few decades. RMM is a powerful tool to have in your arsenal that allows you to have a proactive approach to server maintenance and support from a remote team that is an extension of your department.

Consider your RMM options now before the future catches up with you. Because you cannot scale if your IT infrastructure is holding you back.



For more information please contact one of our consultants:

Toshiba Tec UK Imaging Systems Ltd

Email

info@toshibatec.co.uk

Website

www.toshibatec.co.uk