RMM adoption checklist

RMM solutions enable administrators to control computers, devices, applications, and web access from a remote centralized console.

We've built this comprehensive checklist to guarantee that your RMM solution is configured optimally and delivers maximum value. Check it out to get the most out of your RMM solution.

Planning and preparation

- [ ] Assess the current IT infrastructure and identify the gaps in device management and security that an RMM solution can help resolve.
- [ ] Determine the specific goals and objectives of implementing an RMM solution, such as enhancing device visibility, reducing downtime, and strengthening security.
- [ ] Create a list of devices and systems that require monitoring and management.

Choosing an RMM solution

- [ ] Check out different solutions that provide remote monitoring and management capabilities and compare them based on factors like cloud support, pricing, scalability, and others.
- [ ] Find a solution that best meets the organization's requirements.

- [ ] Ensure that the selected RMM solution is compatible with the organization's existing hardware and software systems.

Implementation plan and pilot phase

- [ ] Develop a project timeline for various phases of the implementation process, such as configuration, testing, and deployment.
- [ ] Assign roles and responsibilities for each stage of the project and identify external factors, if any, that may impact the implementation timeline.
- [ ] Deploy the RMM solution to a small number of selected devices as the pilot stage.

Testing and validation

- [ ] Conduct thorough testing on various aspects such as security, performance, compliance, and user satisfaction.
- [ ] Ensure that the RMM solution is working as intended and is properly identifying security risks.
- [ ] Validate whether the RMM solution is giving you complete and accurate reports and alerts.

Full-scale deployment

- [ ] Deploy the RMM solution across all the selected devices and systems.
- [ ] Ensure that the solution is successfully installed across the entire fleet.

- [ ] Communicate with end users about the new RMM solution and provide training as needed.

Monitoring and management

- [ ] Regularly monitor key RMM metrics to identify potential issues, security threats, or performance concerns.
- [ ] Establish a procedure for addressing issues and threats detected by the RMM solution and automating remedial actions.

Maintenance and updates

- [ ] Ensure that the RMM software and agents are updated to the latest version to ensure optimal performance and security.
- [ ] Regularly perform maintenance activities such as backups, database optimization, and updating device inventory.
- [ ] Review and refine the RMM policies and settings regularly based on end-user feedback and changing business requirements.