



# 10 critères à prendre en compte dans le choix d'une solution RMM

Vous cherchez une solution RMM, mais vous ne savez pas comment faire votre choix ?

Voici une liste de critères à prendre en compte dans votre recherche.

**1.**  **Visibilité** Votre solution RMM vous permet-elle de visualiser tous les appareils (postes de travail, serveurs, périphériques réseau) depuis une seule interface ? Les rapports sont-ils intuitifs ?


**Avantage :** Évitez les erreurs et fournissez un service proactif à vos clients.

**2.**  **Automatisation** Vous permet-elle d'automatiser les tâches courantes, répétitives ? La mise en œuvre est-elle simple ?

**Avantage :** Effectuez plus de tâches sans augmenter vos effectifs.

**54 %**


des employés pensent pouvoir gagner 240 heures par an avec l'automatisation<sup>1</sup>.

**3.**  **Gestion des mises à jour automatisée.** Peut-elle installer automatiquement des correctifs sur des systèmes d'exploitation et des logiciels tiers ?

**Avantage :** Gardez les logiciels à jour afin d'empêcher les cyberattaques.

**27 %**


des entreprises victimes d'une violation de données déclarent avoir été ciblées en raison de vulnérabilités connues non corrigées<sup>2</sup>.

**4.**  **Antivirus puissant, simple à déployer.** Votre solution RMM permet-elle de déployer un antivirus facilement ? Propose-t-elle des fonctionnalités plus avancées que de simples définitions de virus (par exemple, des analyses comportementales et heuristiques) ?

**Avantage :** Renforcez la protection de vos clients contre les logiciels ou les fichiers malveillants.

**350 000**

nouveaux logiciels malveillants sont créés chaque jour<sup>3</sup>.


**5.**  **Protection intelligente des points de terminaison.** S'appuie-t-elle sur l'intelligence artificielle pour signaler les activités suspectes ?

**Avantage :** Protégez vos clients contre les attaques « zero-day », les menaces connues et les comportements douteux.


Les antivirus basés sur des signatures ne détectent que

**50 %**


des menaces<sup>4</sup>.

**6.**  **Sauvegarde en continu, intégrée.** Propose-t-elle une fonction de sauvegarde intégrée ? Pouvez-vous automatiser la sauvegarde ?


**Avantage :** Permettez à vos clients de rester opérationnels après un incident grâce à une protection avancée des données.

**7.**  **Évolutivité.** La politique de prix est-elle favorable à votre entreprise à tous niveaux ? Le déploiement d'agents sur de nouveaux appareils est-il simple ? Avez-vous la possibilité de commencer par activer les fonctionnalités dont vous avez besoin, puis d'évoluer par la suite ?

**Avantage :** Faites des économies en ne payant que ce dont vous avez besoin – et facilitez la croissance de votre entreprise.

**8.**  **Intégrations transparentes.** Quels logiciels votre solution RMM prend-elle en charge ? Permet-elle une intégration avec des logiciels de PSA ? Des API sont-elles prévues pour effectuer d'autres intégrations ?

**Avantage :** Gagnez en efficacité sans changer votre flux de travail.

**9.**  **Accès à distance rapide, sécurisé.** Combien de temps vous faut-il pour vous connecter à une machine distante ? L'accès à distance se fait-il via des protocoles sécurisés ?

**Avantage :** Gagnez du temps et de l'argent en corrigeant les problèmes sans quitter votre bureau.

**10.** **Accompagnement sur le long terme.** Choisissez une solution qui favorise la croissance de votre entreprise en vous donnant accès à des formations, des événements professionnels, ainsi qu'à un support technique convivial.

**Avantage :** Bénéficiez des conseils et du soutien des leaders de l'industrie.



<sup>1</sup> « 2020 In(Sight) Report », WorkMarket. [https://content.workmarket.com/2020-insight-report-what-ai-automation-mean-for-work/?utm\\_source=forbes&utm\\_medium=blog&utm\\_campaign=2017\\_automation\\_report&utm\\_content=home-page](https://content.workmarket.com/2020-insight-report-what-ai-automation-mean-for-work/?utm_source=forbes&utm_medium=blog&utm_campaign=2017_automation_report&utm_content=home-page) (En anglais, consulté en décembre 2019).  
<sup>2</sup> « Patch Now or Pay Later: Report », Forbes. <https://www.forbes.com/sites/taylorarmerding/2019/06/06/report-if-you-dont-patch-you-will-pay/#3117fa383acd> (En anglais, consulté en décembre 2019).  
<sup>3</sup> « Malware », AV-TEST. <https://www.av-test.org/fr/statistiques/logiciels-malveillants/> (consulté en décembre 2019).  
<sup>4</sup> « Only Half of Malware Caught by Signature AV », DarkReading. <https://www.darkreading.com/threat-intelligence/only-half-of-malware-caught-by-signature-av/d/d-id/1336577> (En anglais, consulté en décembre 2019).

## À propos de SolarWinds RMM

SolarWinds® RMM est une plateforme de gestion et de supervision à distance performante, simple d'utilisation, qui évolue selon vos besoins. Démarrez un essai gratuit de 30 jours à l'adresse :

<https://www.solarwindsmisp.com/fr/produits/remote-management/essai>

Les marques de commerce, marques de services et logos de SolarWinds et SolarWinds MSP sont la propriété exclusive de SolarWinds MSP UK Ltd. et de ses filiales. Toutes les autres marques de commerce appartiennent à leurs propriétaires respectifs.

© 2020 SolarWinds MSP Canada ULC et SolarWinds MSP UK Ltd. Tous droits réservés.