



MSP RMM

PATCH MANAGEMENT

BEDROHUNGEN MIT STETS AKTUELLER SOFTWARE VERMEIDEN

Ein Teil der Aufgabe zur Absicherung des Netzwerks besteht darin, zuverlässig und regelmäßig Patches auf die gesamte Software anzuwenden, die mit Ihrer IT-Umgebung interagiert. Wenn Sie viele Workstations und Server verwalten müssen, kann das Patch-Management schnell sehr komplex werden – und Ihr System potenziell langsam und anfällig für schwerwiegende Sicherheitsrisiken machen.

SolarWinds® MSP Remote Monitoring & Management (MSP RMM) optimiert das Patch-Management, indem es Ihnen ermöglicht, Ihre Patching-Richtlinien über eine zentrale, benutzerfreundliche Konsole detailliert zu steuern. Sie möchten den gesamten Prozess automatisieren, Patches für bestimmte Geräte anpassen oder Patches manuell genehmigen oder ablehnen? Mit MSP RMM können Sie den Job in aller Ruhe erledigen.

MEHR KONTROLLE DURCH EINE ZENTRALE KONSOLE

- **Benutzerfreundliche Konsole** – komplettes Patch-Management aus einer zentralen, einfach zu bedienenden Oberfläche.
- **Automatisierung** – automatisches Genehmigen von Patches für bestimmte Programme auf der Basis von Sicherheitsstufen.
- **Planung** – Konfigurieren von Patching-Zeitfenstern zur Aktualisierung von Software, ohne die Mitarbeiter in Zeiten hoher Produktivität zu stören.
- **Anpassbare Richtlinien** – Anwenden von benutzerspezifischen Einstellungen für einzelne Geräte nach Bedarf.

MEHR SOFTWARE AKTUALISIEREN UND SCHÜTZEN

- **Patches für die meiste Unternehmenssoftware** – über 80 Anwendungsfamilien, u. a. Apple, Google, Java, Adobe, Zip-Tools, Skype und Yahoo Messenger.
- **Unterstützung für Microsoft-Produkte** – kontinuierliche Updates für Microsoft Windows, Exchange, Office 365 und mehr zusätzliche

- **Sicherheit für häufig betroffene Programme** – die neuesten Sicherheits-Patches für anfällige Programme wie Adobe und Java.

VON ZUSÄTZLICHEN FUNKTIONEN PROFITIEREN

- **Optimierte Patch-Genehmigung** – Patches im Batch für verschiedene Standorte, Netzwerke, Server und Workstations genehmigen.
- **Patch-Rollback** – Machen Sie Microsoft-Patches einfach auf einem oder mehreren Geräten gleichzeitig rückgängig, wenn sich diese ungünstig auswirken.
- **Automatisierte Aktualisierungen für deaktivierte Geräte** – Niemals ein Update für Geräte verpassen, die während eines standardmäßigen Patch-Management-Zeitfensters deaktiviert waren.
- **Tiefen-Scans zur Aufspürung neuer Schwachstellen** – Tiefen-Scans nutzen, um neue Quellen für Risiken oder Ineffizienzen im Netzwerk zu ermitteln.

PATCHES FÜR WEITVERBREITETE SOFTWARE

Unter anderem für:

- Microsoft Office 365, Exchange, SQL Server, Internet Explorer und Windows, Java, Adobe, Mozilla Firefox, Google Chrome, Apple iTunes und Apple QuickTime.