BR-Systems

MANAGED IT & OPERATIONS 2026

# IT-Infrastruktur unter Kontrolle

## Remote Monitoring & Management als Managed Service — proaktive Überwachung, Patch-Management und Reporting auf eigener Infrastruktur in Deutschland

| | |
|---|---|
| Dokument-ID | BR-WP-RMM-010 |
| Version | 1.0 |
| Fachstand | 27. Juni 2026 |
| Veröffentlicht | 11. Juli 2026 |
| Klassifizierung | Öffentlich – kostenfreier Fachbeitrag |
| Autor | Benjamin Raulf, BR-Systems |
| Herausgeber | BR-Systems · IT-Systemhaus · Unterlüß |
| Standort zum Fachstand | Unterlüß |
| Kontakt | info@br-systems.eu · https://br-systems.eu · +49 179 1601700 |

# Executive Summary

Dieses Whitepaper beschreibt Managed RMM als betriebenen Service von BR-Systems: von der Ausgangslage über Leistungsumfang und Preismodell bis zu Sicherheit, Grenzen und praktischen Anwendungsfällen. Im Mittelpunkt stehen Transparenz, planbare Kosten und ein fester Ansprechpartner — nicht ein anonymes Ticketsystem.

**Die vier wichtigsten Aussagen**

- Proaktives Monitoring statt reaktiver Fehlerbehebung
- Ein Paket, ein Preis pro Endpunkt — ohne Basic-/Premium-Stufen
- Alerts werden von BR-Systems bewertet, nicht nur weitergeleitet
- Klare Abgrenzung: Monitoring ist nicht gleichbedeutend mit 24/7-Support

## Inhalt

# 1. Ausgangslage: Wenn IT erst auffällt, wenn etwas ausfällt

In vielen mittelständischen Unternehmen wird IT nach dem Prinzip „läuft doch“ betrieben. Festplatten laufen voll, Updates stehen aus, Backup-Jobs scheitern unbemerkt und Dienste fallen erst auf, wenn Mitarbeitende sich melden. Reaktive Fehlerbehebung kostet Zeit, Geld und Vertrauen — besonders dann, wenn kein aktuelles Inventar, keine dokumentierten Wartungsfenster und keine klaren Eskalationswege existieren.

Remote Monitoring & Management (RMM) verschiebt den Fokus von reiner Störungsbearbeitung zu einem betriebenen Überblick: CPU, RAM, Speicher, Dienste, Patches, Inventar und Konfigurationsänderungen werden kontinuierlich erfasst. BR-Systems betreibt die Plattform auf eigener Infrastruktur in Deutschland und übernimmt Einrichtung, laufende Pflege sowie die fachliche Bewertung eingehender Meldungen. Für Kunden entsteht damit Transparenz über den Zustand ihrer Umgebung — ohne dass sie eine eigene Monitoring-Abteilung aufbauen müssen.

Managed RMM ersetzt weder eine durchdachte Sicherheitsarchitektur noch einen dedizierten Helpdesk. Es schafft jedoch die technische und organisatorische Grundlage, um Probleme früher zu erkennen, Wartung planbar durchzuführen und Entscheidungen auf nachvollziehbaren Daten zu treffen. Gerade in Umgebungen mit wenigen internen Ressourcen ist das der Unterschied zwischen „wir merken es irgendwann“ und „wir wissen es rechtzeitig“.

# 2. All-in-One-Leistungsumfang ohne Stufenmodell

BR-Systems bietet Managed RMM als ein Paket an — ohne Basic- oder Premium-Stufen, bei denen zentrale Funktionen erst im teureren Tarif freigeschaltet werden. Monitoring, Patch-Management, Fernzugriff, Inventar, Automatisierung und Reporting gehören zum vereinbarten Leistungsumfang. Die konkrete Ausgestaltung — etwa Wartungsfenster, Alert-Schwellen, Rollen und Berichtsintervall — wird im Projekt festgelegt und dokumentiert.

Typische Bausteine umfassen die Überwachung von Servern, Arbeitsplätzen und ausgewählten Netzwerkgeräten; zentrales Patch-Management nach Schweregrad; Fernzugriff auf Desktop, Shell und Dateien innerhalb definierter Berechtigungen; Software- und Hardware-Inventar; Skripte und Automatisierung für wiederkehrende Aufgaben; sowie Statusberichte für Geschäftsführung oder Prüfer. Unterstützt werden Windows, macOS und Linux — abhängig von der jeweiligen Umgebung und dem vereinbarten Scope.

Entscheidend ist der Betrieb: Alerts werden nicht blind an Kunden weitergeleitet. BR-Systems priorisiert Meldungen, ordnet sie fachlich ein und leitet bei Bedarf Maßnahmen ein. So bleibt der Kanal verständlich und Eskalationen nachvollziehbar. Ein Dashboard allein schafft noch keinen stabilen Betrieb — erst Bewertung, Dokumentation und definierte Reaktionswege machen Monitoring wirksam. Reports über Patch-Status, Inventar und Systemzustand können zudem als Grundlage für interne Reviews, ISMS-Dokumentation oder Kundennachweise dienen — sofern im Projekt vereinbart.

# 3. Preismodell: transparent und volumenorientiert

Das Preismodell ist volumenorientiert: ein Nettopreis pro Endpunkt und Monat, unabhängig davon, ob es sich um einen Arbeitsplatz oder einen Server handelt. Es gibt keine Mindestlaufzeit. Die Staffel richtet sich nach der Gesamtzahl verwalteter Endpunkte — nicht nach einzelnen Standorten oder getrennten Verträgen, sofern nicht ausdrücklich anders vereinbart.

Bei jährlicher Vorauszahlung werden elf Monate berechnet — ein Monat entfällt als Preisvorteil. Alle Angaben verstehen sich netto. Zusatzleistungen wie Projektarbeiten, Vor-Ort-Einsätze oder Erweiterungen außerhalb des vereinbarten Serviceumfangs werden separat angeboten. So bleibt der laufende Betrieb planbar, ohne versteckte Stufen oder Funktionsausschlüsse.

Vor Vertragsabschluss wird die Endpunktanzahl gemeinsam ermittelt und der passende Staffelpreis schriftlich bestätigt. Wächst die Umgebung, wird die Staffel angepasst — transparent und nachvollziehbar. Ein kurzes Erstgespräch klärt Ausgangslage, gewünschten Umfang und Erwartungen an Reaktionszeiten, ohne Produktdruck.

# 4. Typische Anwendungsfälle in der Praxis

KMU mit verteilten Standorten profitieren von einer zentralen Übersicht aller PCs und Server, geplanten Wartungsfenstern und Fernsupport ohne Anfahrt. Praxen und Kanzleien erhalten dokumentierte Änderungen, nachvollziehbare Patch-Stände und klare Eskalationswege — wichtig dort, wo Verfügbarkeit und Nachweisbarkeit eine Rolle spielen. In Produktion und Technik überwachen automatische Checks kritische Dienste, Speicher und Backup-Jobs und warnen vor Engpässen, bevor ein Prozess stillsteht.

IT-Abteilungen mit Personalmangel nutzen Managed RMM als Entlastung bei Monitoring, Inventar und Patch-Routinen. BR-Systems übernimmt die technische Erfassung und erste Bewertung; interne Teams können sich auf Projekte und Fachanwendungen konzentrieren. Auch MSP-nahe Szenarien mit mehreren Mandanten lassen sich über Gruppen und Rollen strukturieren — stets mit dokumentierter Trennung und vereinbarten Zuständigkeiten.

Drei Praxisbeispiele verdeutlichen den Nutzen: Ein Betrieb mit 45 Arbeitsplätzen und zwei Servern erkannte nach Einführung früh drei drohende Festplattenprobleme und rollte Updates nach Feierabend aus. Ein Dienstleister mit acht Kunden und 95 Geräten reduzierte Vor-Ort-Termine deutlich durch zentrale Oberfläche und Remote-Zugriff. Eine Organisation mit Compliance-Anforderungen nutzt automatische Reports über Patch-Compliance und Systemzustand als Grundlage für ISMS-Dokumentation.

# 5. Sicherheit, Datenschutz und Integrationen

Die Agent-Kommunikation erfolgt TLS-verschlüsselt. Verarbeitung und Auftragsverarbeitung orientieren sich an den Anforderungen der DSGVO; eine AVV wird auf Anfrage bereitgestellt. Mandantentrennung erfolgt über Gruppen und Rollen. Hosting und Betrieb liegen in Deutschland durch BR-Systems — ohne Weitergabe an unbefugte Dritte.

Die Plattform unterstützt ergänzende Integrationen für Fernzugriff, Security und Ticketing — etwa AnyDesk, TeamViewer, RustDesk, Bitdefender, Grafana oder Zammad. Welche Module sinnvoll sind, hängt von der bestehenden Umgebung ab. Nicht jede Integration ist in jedem Projekt erforderlich; Ziel ist ein schlanker, wartbarer Gesamtprozess.

Sicherheit endet nicht an der Plattformgrenze. Zugänge werden nach dem Prinzip der geringsten Rechte vergeben, administrative Konten getrennt geführt und Änderungen dokumentiert. Regelmäßige Reviews prüfen, ob Alerts, Wartungsfenster und Berechtigungen noch zur realen Nutzung passen.

# 6. Abgrenzung: Monitoring vs. 24/7-Support

Die Plattform kann vereinbarte Messwerte rund um die Uhr automatisiert erfassen. Das bedeutet nicht, dass jede Meldung sofort von einer Person bearbeitet wird. Bearbeitung und Reaktion erfolgen innerhalb der im Servicevertrag festgelegten Zeiten und Eskalationswege. Managed RMM ist kein Ersatz für einen dedizierten 24/7-Helpdesk — es schafft jedoch Transparenz und frühere Erkennung von Problemen.

Kunden sollten vor Vertragsbeginn klären, welche Reaktionszeiten sie erwarten, welche Kanäle für Eskalation gelten und welche Aufgaben im vereinbarten Umfang liegen. Ein klarer Service-Scope verhindert Missverständnisse zwischen „System hat gemeldet“ und „Problem ist gelöst“. BR-Systems legt diese Grenzen offen — im Whitepaper, im Angebot und im laufenden Betrieb.

# 7. Vom Konzept zum belastbaren Betrieb

Technische Maßnahmen entfalten ihren Wert erst in einem geregelten Betrieb. Dazu gehören ein benannter Service Owner, eine aktuelle Systemdokumentation, ein Änderungsprozess und ein fester Kontrollrhythmus. Der Umfang darf zur Organisation passen — ein kleiner Betrieb benötigt keine Konzernbürokratie, aber Klarheit darüber, wer entscheidet, wer umsetzt und wer prüft.

Bei jeder Maßnahme sollten vier Fragen beantwortet werden: Welches konkrete Risiko wird reduziert? Woran erkennen wir, dass die Maßnahme aktiv ist? Wer reagiert auf Fehler oder Alarme? Wie verlassen oder ersetzen wir die Lösung später? Diese Fragen machen Angebote vergleichbar und erleichtern die Übergabe zwischen internen und externen Verantwortlichen.

Dokumentation ist kein Selbstzweck. Sie verkürzt Störungen, macht Änderungen sicherer und verhindert, dass kritisches Wissen ausschließlich bei einer Person liegt. Gute Dokumentation ist knapp genug, um gepflegt zu werden, und konkret genug, um in einer Störung zu helfen.

Ein Management-Review sollte Risiken nicht in technischen Einzelmeldungen verstecken. Sinnvoll sind wenige verständliche Kennzahlen: ungeklärte kritische Schwachstellen, erfolgreiche Restore-Tests, überfällige Updates auf kritischen Systemen und offene Maßnahmen nach Priorität.

Die beste Roadmap ist umsetzbar. Maßnahmen werden in kleine, prüfbare Pakete geschnitten und mit Termin sowie Verantwortlichem versehen. Nach jedem Abschnitt wird geprüft, ob der Betrieb tatsächlich stabiler geworden ist.

# Preismodell im Überblick

Alle Preise netto pro Endpunkt und Monat. Jährliche Zahlweise: elf Monate Vorauszahlung. Online-Kalkulation unter https://br-systems.eu/rmm-monitoring.html#rmm-kalkulator

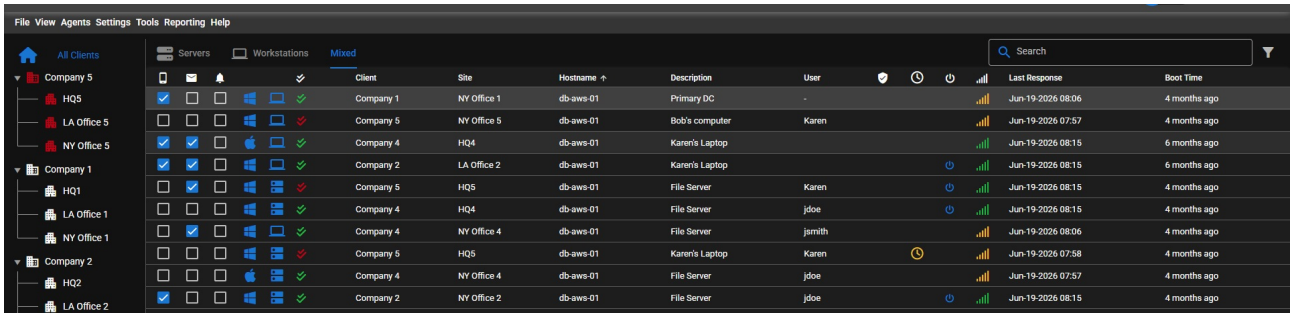
| Endpunkte (netto / Monat) | Preis |
|---|---|
| 1 – 9 Endpunkte | 9,90 EUR |
| 10 – 24 Endpunkte | 8,00 EUR |
| 25 – 49 Endpunkte | 6,90 EUR |

| | |
|---|---|
| 50 – 99 Endpunkte | 5,00 EUR |
| 100 – 179 Endpunkte | 4,50 EUR |
| 180 – 299 Endpunkte | 4,00 EUR |
| 300+ Endpunkte | 3,50 EUR |

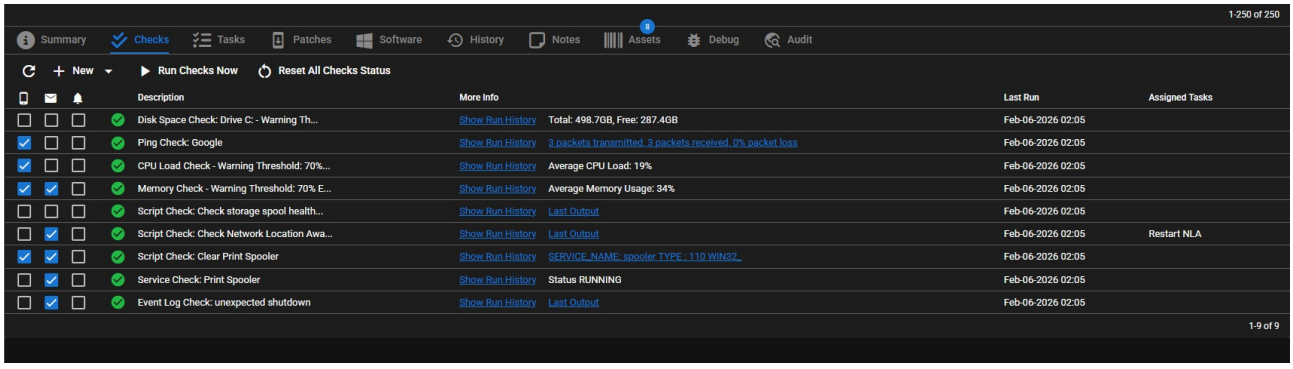
# Plattform-Einblicke

Die folgenden Auszüge zeigen typische Oberflächen für Übersicht, automatische Prüfungen und Patch-Management. Betrieben und betreut durch BR-Systems auf eigener Infrastruktur in Deutschland.

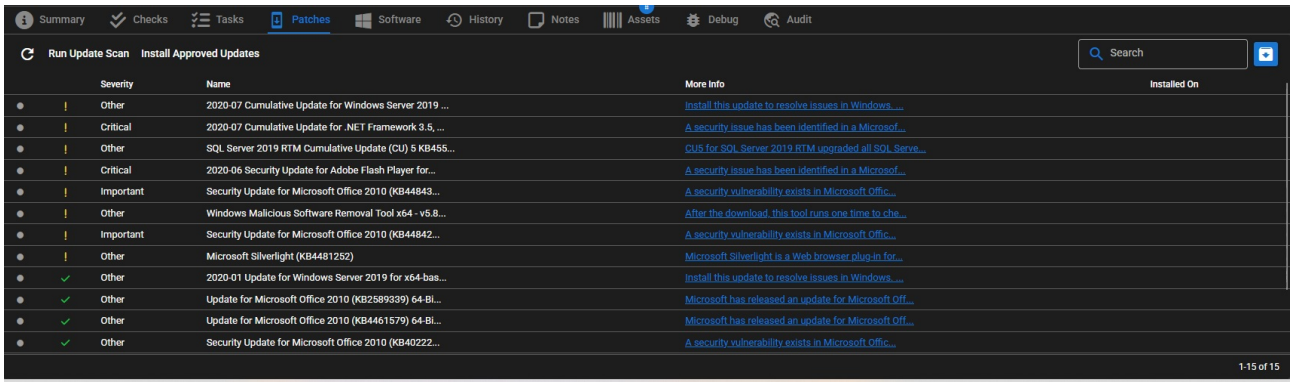
## Abb. 1: Zentrale Übersicht aller verwalteten Systeme




## Abb. 2: Automatische Prüfungen — Festplatte, CPU, RAM, Dienste und Event Logs




## Abb. 3: Patch-Management nach Schweregrad




### Praxis-Checkliste

- Kritische Systeme und Endpunkte vollständig inventarisieren
- Gewünschte Reaktionszeiten und Eskalationswege schriftlich festlegen
- Wartungsfenster für Patches und Neustarts abstimmen
- Rollen und Fernzugriffsberechtigungen nach Bedarf modellieren
- Alert-Schwellen und Prioritäten gemeinsam definieren
- Quartalsweise prüfen, ob Reports und Monitoring zum Alltag passen
- Restore-, Backup- und Sicherheitsmaßnahmen unabhängig vom RMM bewerten

# Fazit

Managed RMM macht den Zustand Ihrer IT sichtbar und Wartung planbar — wenn Scope, Reaktionswege und Verantwortlichkeiten klar vereinbart sind. BR-Systems unterstützt bei Bestandsaufnahme, Einführung und laufendem Betrieb — herstellerbewusst, aber nicht verkaufsgetrieben.

# Quellen und weiterführende Informationen

[1] BR-Systems: Managed RMM & Kalkulator
https://br-systems.eu/rmm-monitoring.html

[2] BR-Systems: Managed IT & RMM-Leistungen
https://br-systems.eu/managed-services.html

[3] BSI: Informationen und Empfehlungen für KMU
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/KMU/kmu_node.html

Historischer bzw. fachlicher Bezugsstand: 27. Juni 2026. Veröffentlicht: 11. Juli 2026. Online-Quellen zuletzt geprüft: 27. Juni 2026. Der Fachstand ist kein vorgetäuschtes Veröffentlichungsdatum. Dokument-ID BR-WP-RMM-010, Version 1.0.

### Über BR-Systems

- Managed RMM, Microsoft 365, Security, Proxmox, Backup und Netzwerk aus einer Hand
- Betrieb auf eigener Infrastruktur in Deutschland mit festem Ansprechpartner
- Transparente Preise, dokumentierte Änderungen und nachvollziehbare Eskalation

## Nächster Schritt

Sie möchten prüfen, ob Managed RMM zu Ihrer Umgebung passt? BR-Systems klärt Ausgangslage, Endpunktanzahl und gewünschten Betriebsumfang — ohne Produktdruck. Kontakt: info@br-systems.eu oder +49 179 1601700 · https://br-systems.eu/rmm-monitoring.html