Service Definition – Datto RMM Managed Endpoint (Kaseya 365)

This document describes how the service works and is intended for publication on the Digital Marketplace service page. It does not include pricing.

Document version: 1.0

Last updated: 30 January 2026

Supplier: Kent MSP Ltd

Service name: Datto RMM Managed Endpoint (managed)

1. What the service is

Datto Remote Monitoring and Management (RMM) provides centralized, cloud-managed endpoint monitoring, patching, security enforcement, automation, and remote support. Customers access a secure web interface to manage devices, apply policies, and remediate issues. Where agreed, we provide a managed service wrapper (monitoring, alert handling, and support) and operate the tenant on the customer's behalf.

1.1 Core capabilities

- Real-time monitoring, alerting, and inventory across supported endpoints (Windows, macOS, Linux, and network devices via SNMP).
- Patch and software management for operating systems and third-party applications.
- Security and compliance tooling including antivirus management, EDR integrations, and policy enforcement.
- Remote access, remote PowerShell/terminal, and scripted automation at scale.
- Dashboards, reports, and audit trails within the Datto RMM web interface.

2. Service interface

The service is administered through a secure, browser-based Datto RMM web interface. Users authenticate with assigned accounts; single sign-on via KaseyaOne can be enabled. Role-based access control limits capabilities (for example, read-only admin, site admin, and technician roles). Version updates are delivered centrally by the SaaS platform.

3. Endpoint management and automation

3.1 Monitoring and alerting

- Device monitoring policies with thresholds and intelligent alerts (CPU, memory, disk, services, security state).

- Automated ticket creation when integrated with PSA (e.g., Autotask).

3.2 Patch & software management

- Windows Update policy and third-party patching via Software Management.
- Maintenance windows and reboot behaviour configurable per policy.

3.3 Remote access & remediation

- Secure remote control, Web Remote PowerShell/terminal, and file transfer.
- Jobs and Components (installers, scripts, monitors) for at-scale remediation.

4. Onboarding

- Tenant setup, SSO configuration (optional), and administrative access.
- Discovery and agent deployment planning (package, script, or network deployment).
- Policy design (monitoring, patching, maintenance windows, security baselines).
- Initial rollout and validation (sample devices, alert tuning, remote access test).
- Handover of admin guidance and operational runbooks.
- On-site assistance can be provided where agreed as an additional service.

5. Offboarding and end-of-contract

- Agree an offboarding plan and timeline (including report/export requirements).
- Suspend changes and preserve configuration during the offboarding window (if required).
- Export device inventories, configurations, and logs using built-in reports/CSV exports.
- Remove agents from devices and revoke credentials/SSO trusts when instructed.
- Upon request, delete the tenant to remove service data retained by the platform (irreversible).

6. Service constraints

- Cloud-hosted SaaS: release cadence and feature availability are managed centrally by Datto.
- Agent is required for full endpoint management; network-only devices are monitored via SNMP with limited functions.
- Some features and integrations may vary by region and account entitlements (e.g., Kaseya 365 tier).

7. Service levels

7.1 Availability

The platform is delivered as a multi-tenant cloud service with published availability targets by the vendor. We provide operational monitoring and incident handling aligned to the support level purchased.

7.2 Support hours and response targets

- P1 (Critical): 15–60 minutes
- P2 (High): within 4 hours
- P3 (Medium): within 1 business day
- P4 (Low): within 2–5 business days

Support hours and escalation routes are set out in the service order or managed service agreement.

8. After-sales support

- Incident management and service request handling via ticket, email, and phone (where included).
- Proactive monitoring (where included) for policy failures and capacity-related alerts.
- Regular service reviews (where included) and reporting exports on request.
- Vendor escalation to Datto/Kaseya where required.

9. Technical requirements

- Supported operating systems for protected endpoints (Windows, macOS, Linux) per Datto RMM documentation.
- Sufficient local resources for the Datto RMM agent (disk, CPU, RAM appropriate to enabled features).
- Reliable outbound internet connectivity to Datto RMM cloud endpoints; allowlisting of required domains/ports.
- Administrative rights for agent installation and remote tools where applicable.

10. Outage and maintenance management

- Operational alerts visible within the Datto RMM console (e.g., agent health, policy status).
- We notify customers of planned maintenance where it may impact service and coordinate incident communications.
- Datto publishes release notes/status information; we track releases and validate changes as part of managed operations.

11. Hosting options and locations

The service is delivered from Datto-managed cloud infrastructure. No customer-hosted management servers are required. Data residency and platform regions are determined by the Datto provisioning region for the tenant. Remote access sessions and telemetry flow through Datto's cloud services.

12. Access to data

- Administrators can export device inventories, audit data, and reports (CSV/PDF) from the web interface.
- Configuration and policy definitions can be documented/exported via reports and screenshots where needed.
- At contract end, data extraction is achieved through scheduled reports/exports prior to tenant deletion.

13. Security

13.1 Access control

- Role-based access control with granular permissions for global and site scopes.
- Multi-factor authentication via KaseyaOne and platform login options.
- Tenant separation enforced in a multi-tenant model.

13.2 Data protection

- Encryption in transit for agent and console communications.
- Session controls and audit logging available via the platform.

13.3 Vulnerability management and patching

We operate a risk-based vulnerability management process across our managed environments and supporting systems, prioritising remediation for actively exploited issues and applying an update-by-default approach.

13.4 Protective monitoring and incident response

- Layered protective monitoring for service anomalies and security-relevant events.
- Documented incident response (detect, triage, contain, eradicate, recover, lessons learned) with reports for confirmed incidents.

14. Accessibility

This document is provided in an accessible format with structured headings and lists. If you require an alternative format (for example, large print), please contact us via our support channels.