eBook

datto

Datto RMM

A Security-First Solution

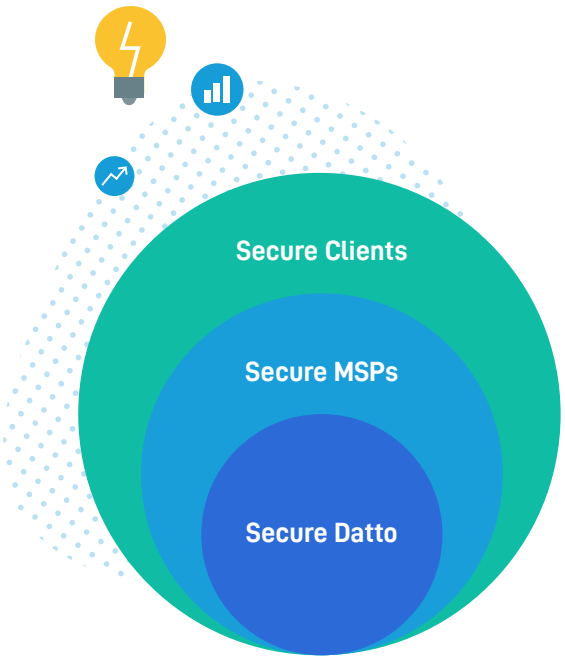
Comprehensive Security Not Complex Security

77% of SMBs believe their IT environments have become more complex over the past two years, and 52% of SMBs believe that this complexity is driving a rapid change in the cybersecurity landscape[1].

Securing clients' endpoints, monitoring new devices, and patch management are just a few of ongoing tasks that MSPs perform to keep their clients secure against a continuously evolving cyber-threat landscape.

Tackling complex security challenges at scale demands a comprehensive approach that builds on sound security fundamentals and brings together scalable frameworks and processes. Datto RMM creates a robust, yet easy to manage security ecosystem for the product, MSPs, and their clients by taking a multi-layered approach.

[1] Sharp - The Vulnerable State of SMB Cybersecurity and How Managed Service Providers Can Help



A Multifaceted Approach To Building a Secure RMM

Datto RMM is modeled to maximize protection against multiple threat vectors across the cyberattack surface. As part of our comprehensive security approach, Datto RMM works to achieve three key objectives:

- **Securing Datto RMM**: At Datto, security starts with us, and we do the utmost to protect our infrastructure and applications through a combination of advanced processes, frameworks, and product culture.
- **Securing MSPs**: With a tool as mission-critical and powerful as RMM, the platform's security is paramount. Hence, Datto RMM is designed to thwart any attempt to harm the MSP infrastructure through the RMM platform.
- **Enabling MSPs to secure their clients**: Datto RMM provides MSPs deep visibility into endpoints, allowing them to take strong proactive security measures and stay ahead of security challenges.

Securing Datto RMM

Built on of our security-first culture, Datto RMM leverages secure development processes and periodic stringent information security assessments. Other proactive measures include:

- **Cloud from day one**: On-premise versions of RMM have been vulnerable to security breaches over the past few years, especially when IT environments are becoming increasingly complex and diverse. Datto RMM has always been a cloud-based solution, making it a more secure choice with a reduced attack surface.
- Datto RMM's **highly-experienced product development team** constantly scans the technology landscape for new ways to enhance product security.
- Datto RMM **source code is retained in separate secure repositories** that are only accessible through Datto's internal network with its own Multifactor authentication (MFA) required to access it.

- We have **a strict code review process** where any new code submission is reviewed by a minimum of two additional developers.
- **Multiple QA (Quality Assurance) passes** throughout the lifecycle of the product's development from sandbox to maintenance, test, and staging environments. After every update, the software production environment has a very strict QA pass, including security tests and attack simulations.
- We perform **code reviews and dependency scanning** to ensure that our application and its dependencies are secure.
- Datto RMM has been **certified by independent auditors to meet SOC II Type II** requirements with the Security and Availability Trust Services Criteria. These audits are conducted every year to ensure that we stay compliant with the requirements.

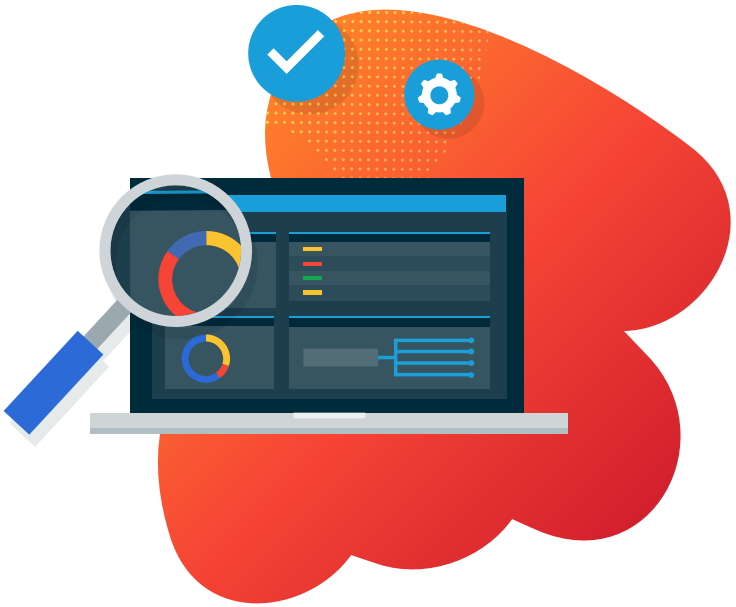
Did you know?

Datto RMM was ranked in the top 20% of all companies undergoing their Building Security In Maturity Model (BSIMM) assessment, an independent third-party security assessment of software applications based on a widely-accepted maturity model. The only MSP-focused company to participate, Datto RMM is the only channel RMM evaluated to date. Going forward, any new participants will be benchmarked against Datto and a list of well-known enterprise companies.

Securing MSPs

When it comes to securing their infrastructure, MSPs have a lot at stake. They should evaluate the security posture of their RMM vendor to ensure that they prioritize security. Datto RMM has several built-in security measures that are designed to prevent any attempt by bad actors to weaponize the RMM platform against MSPs.

- Datto RMM operates on **multiple resilient, high-availability, scaling platforms** hosted within Amazon Web Services (AWS).
- Our RMM is hosted on **AWS virtual private cloud**, isolated from the public cloud environment and in different regions globally. Each cloud instance is replicated, and even load balanced across a minimum of two data centers.
- **Advanced access to the production environment is available only to a limited few authorized employees** and must be signed off by another employee at every instance. Access to the MSP's RMM instance must be approved by them.
- Datto RMM has **regular reviews with AWS** to sharpen our hosting security measures and minimize the risk of a security incident.
- **All data transferred between Datto RMM, the users, and the endpoints is encrypted.** The data centers are firewalled. The product is regularly penetration-tested by professionals outside the company, and, in the event of a discovery, a fix is prepared and generally released outside of scheduled release windows.



- **SSH and RDP remote access to Datto RMM infrastructure is disabled** to further enhance back-end security.
- **Access to AWS instances is controlled through independent security groups**, firewall groups for front-end, back-end, and data repositories, etc.
- Datto RMM employs a **web application firewall (WAF)** in front of all of our services.
- We use a **managed detection and response (MDR) solution across Datto RMM infrastructure** to look for suspicious or non-conformant behavior.
- Datto RMM **ComStore Components are carefully managed and tested** with the RMM team, with only a select and audited group of staff given access to manage ComStore Components. Components are not automatically updated in our partners' tenants; we allow partners to view and approve updates to ComStore Components individually, and the contents can be inspected by copying the component.

Did you know?

Competing RMM products have often focused on on-premises RMM operations, which places a significant workload on IT staff to ensure that systems are performing and running the latest versions of applications, integration plug-ins, security certificates, etc. In the past, security incidents have been reported in on-premises RMM products involving out-of-date plug-ins causing breaches and expiring security certificates causing software malfunctions.

In contrast, Datto RMM is a pure cloud-based solution, with all configuration and data held securely in AWS data centers. Datto manages security certificates; similarly, there are no plug-ins or add-ons to worry about as everything is handled by the cloud servers running the Datto RMM product. In case of a security issue, the product can be patched instantaneously.

Enabling MSPs to Secure Their Clients

Small and medium businesses increasingly trust MSPs to manage their IT infrastructure and keep them secure. Datto recommends a comprehensive security strategy that utilizes the multiple avenues of endpoint and IT security that Datto RMM offers, including:

- **Several controls to secure managed endpoints are provided to MSPs by Datto**. These controls are also outlined in our Security Best Practices article.
- **Device/agent security** ensures that any new device will require administrator approval to run jobs, download components, and implement device policies.
- **Agent encryption between the device and main console**: A unique encryption key is assigned to every agent installation to authenticate communication between the agent and the platform, avoiding any attempt to impersonate the agent.
- **IP address restriction**: Control who uses the agent browser and the UI by allowing only select IP addresses to access these interfaces.
- **Windows update statuses (patch management)**: Datto RMM works with Windows to immediately report issues with the Windows Update service. Furthermore, Datto RMM's robust patch management core is fully compatible with Windows 10 and Windows 11 and will report any issues installing updates using the same interface.
- **3rd party software updates and status** ensures critical internet-connected apps installed on endpoints are kept up to date seamlessly.
- **Security audit**: Datto RMM provides a component called "Security Audit [WIN]" that helps MSPs identify the right security policy for their network and how many devices deviate from this policy. The audit evaluates devices based on various criteria across different categories such as operating systems, user accounts, network, and device security.

Did you know?

Datto RMM Ransomware Detection monitors for the existence of crypto-ransomware on endpoints using proprietary behavioral analysis of files and alerts you when a device is infected. Upon detection, Datto RMM can isolate the device and attempt to stop suspected ransomware processes to prevent the ransomware from spreading.

- To help you answer these questions, Datto RMM provides a **Security Audit component and monitoring policy set** intended to pinpoint common security concerns on Windows devices. These concerns are raised in the StdOut from the component run and within the Windows Event Log. This information can then be caught by the monitoring policy and filtered. If you are linking to a PSA solution, workflow rules can also be applied to tickets.
- **Agent policies** can be used to configure how much control Datto RMM users are given over endpoints. MSPs can configure how much control users remoting into a device receive, whether devices can receive jobs, and other features. This can be particularly useful for devices that should never run automated jobs or receive remote support.
- Datto RMM has several **admin-level security measures** such as:
  - **Mandatory two-factor authentication (2FA)**: Datto RMM enforces 2FA on all accounts to enable a second level of authentication in addition to login credentials. Both factors of authentication must be used and must be entered correctly in order to establish the user's identity beyond doubt.
  - **IP address restriction**: Consider locking down the user interface, as with the Agent Browser, only to allow logins from IP addresses within an accepted range.
  - **Granular security levels**: Security levels specify and limit users' access when logged in to the Datto RMM web interface, the Agent Browser, or a Web Remote session. Different levels with granular control over access fields can be configured, saved, and assigned to different users. If a group of users needs identical security privileges, these levels can be applied to a list of users.
  - **User activity logging**: Datto RMM's new user interface combines user and device logging into a unified interface where it is possible to query all actions performed by a user and delve deep into their activity pertaining to one or more devices. This enables RMM admins to easily analyze and flag any undesirable user activity.

Get started with a 14-day free trial of Datto RMM