Kaseya

365

COMPONENTS AND ESSENTIAL AUTOMATIONS

TABLE OF CONTENTS

Kaseya 365

MANAGE | ENDPOINT MANAGEMENT

datto | RMM

Kaseya 365

As an intuitive, powerful, and affordable cloud platform, Datto RMM helps MSPs manage the complexity, costs, and risks associated with supporting every device they are contracted to support—from on-premises to cloud-hosted, from server to network device, and everything in between. Whether managing a single endpoint or hundreds of thousands, Datto RMM helps MSPs keep their supported estate secure, patched, stable, and functioning.

NEXT GENERATION RMM FOR THE MODERN MSP

Secure, Scalable, and Always On

As a true SaaS platform, Datto RMM is easily accessible and allows MSPs to focus on managing their customers. The platform's enhanced security posture, with mandatory two-factor authentication, routine penetration testing and infrastructure hardening, and active monitoring for unauthorized access attempts, helps maintain its proven track record of 99.99% uptime. And, since it's a truly scalable, cloud-based platform, there is no limit to the number of devices you can support.

Simple Onboarding, Easy Adoption

Even with a broad, powerful feature-set, Datto RMM is easy to set up, deploy and use with pre-configured functionality, an intuitive user experience, and modern user interface. Having onboarded thousands of MSPs to Datto RMM, Datto has the experience and know-how to support you in every step of the onboarding process, whether you are new to RMM or migrating from an existing RMM platform. Built-in wizards simplify the implementation process by providing contextual product walk-throughs, automatically configuring key features, and delivering comprehensive on-the-job training for your technicians.

In addition, Datto offers a range of accessible resources to help your team fully utilize the platform. From Datto Academy certifications, ongoing education and training, and Datto's award-wi ning, 24/7/365 direct-to-tech support, Datto is committed to helping you start strong and stay strong.

DRIVE EFFICIENCY AND AUTOMATION INTO YOUR SERVICE DELIVERY

Datto RMM has robust, MSP-centric features in a fully-integrated SaaS platform. With monthly release cycles, constant improvement and innovation, Datto RMM is designed to help MSPs support the IT environments of today and prepare for those of tomorrow. Some key features of Datto RMM include:

• Discovery and Asset management: Real-time visibility of every asset under contract—where it is, status, condition, and compliance.

• Monitoring: Know what's going on with every device through realtime notification of alerts and automated responses to reduce device downtime.

• Management: Keep devices secure, patched, and optimized through proactive, centralized, policy-based device management delivering automation at scale.

• Remote Support: Secure, fast remote access to devices with an array of powerful remote support and screen share tools.

• Reporting: Showcase the value you're delivering to clients with scheduled reporting that provides insight on devices, customer health, and activity.

Additionally, Datto RMM includes pre-built monitoring policies and scripts, third-party access rights, wide-ranging integrations into other key platforms such as PSA tools, antivirus, warranties, and documentation management to provide the ideal blend of capability, usability, security, and performance.

FLEXIBLE, AUTOMATED PATCH MANAGEMENT

Datto RMM helps MSPs deliver efficient, effective, policy-based patch management for Microsoft and third-party software, a critical service to maximize security and minimize downtime. It also provides critical compliance information to customers by automating the reporting of patch status and compliance.

AUTOMATION AND SCRIPTING

Whether you are just starting out with RMM or are a mature MSPsupporting tens of thousands of devices, Datto RMM offers a wide range of powerful automation capabilities that are easy to set up and manage. Dynamic device targeting functionality coupled with a flexible scripting engine means you can streamline service delivery with scalable automation. Additionally, the Datto RMM ComStore offers hundreds of free, pre-built scripts and automation policies to streamline your technical support.

REAL-TIME MONITORING

Datto RMM monitors all of your devices in real-time—servers, VMs,ESXi, PCs, laptops, network devices—instantly informing you of current issues and flagging potential problems. Powerful autoresponses to alerts resolve problems automatically or simplify troubleshooting by providing technicians with useful diagnostic information. The ComStore comes complete with dozens of best practice monitoring components to reduce the complexities of monitoring today's complex IT environments.

RMM RANSOMWARE DETECTION

Datto RMM monitors for crypto-ransomware on endpoints using behavioral analysis of files, and receives automatic alerts when a device is infected so the end user doesn't have to report it. Automated responses attempt to kill the ransomware process whileDatto RMM isolates the device automatically to prevent spread of ransomware while still maintaining contact with RMM. This allowstechnicians to take effective action and recover with integrated Datto Continuity products by restoring the impacted endpoint to aprevious state.

RAPID REMOTE SUPPORT

Datto RMM enables your engineers to rapidly and securely connect to any device, regardless of location. Our range of remote support tools enables efficient troubleshooting and assistance without interrupting the end user. Should screen share be required, Datto RMM has its own fast, effective HTML5-based remote control built into the platform, meaning your technicians can access any supported device.

FLEXIBLE REPORTS AND DASHBOARDS

The ability to effectively report to customers on performance, health, and security is critical for MSPs. Datto RMM comes with modern, configurable dashboards that provide insight and understanding, as well as reporting capabilities that provide client-facing reporting on critical metrics, activity, and status. A robust, accessible REST API offers further reporting options.

NETWORK TOPOLOGY MAPPING

Network and IoT devices are everywhere and need to be managed— and managing the network starts with understanding what's out there. Datto RMM's Network Topology Maps help MSPs better manage their clients' networks by continuously discovering and identifying every device on the network, generating a visual layout of the network to show how devices are connected to each other, and quickly identifying where issues are.

INTEGRATIONS AND OPEN ECOSYSTEM

Datto RMM and Autotask PSA are a unified platform. That means synchronized assets, full bi-directional sync of alerts with tickets, integrated data and reporting. Datto RMM is also fully integrated with Datto BCDR and Datto Networking. However, our commitment to an open ecosystem maintains out-of-the-box integrations with a broad range of MSP-centric solutions. The powerful API also allows MSPs to integrate Datto RMM into their other key business systems, further streamlining business processes and data sharing.

MICROSOFT 365 MANAGEMENT

Datto RMM's Microsoft 365 Management feature allows you to integrate both platforms in just a few clicks. Get a comprehensive overview of your tenants, users and associated devices. With the Microsoft 365 universe constantly expanding, routine tasks can turn into long-drawn, error-prone processes. However, Datto RMM's Microsoft 365 Management simplifies such tasks. Not only does this enhancement reduce potential human errors, it also bolsters security and streamlines operations.

SUPPORTED PLATFORMS

Datto RMM operates on Windows, Linux, MacOS, VMWare, and SNMP Devices.

datto | RMM

Kaseya VSA 10 is a power-packed solution designed to help busy IT professionals boost their efficiency by up to 50%. VSA 10 unifies IT management into a single platform, improving IT professionals day-to-day lives and removing the “space between” of endless alt-tabbing between applications.

VSA 10 empowers MSPs and internal IT teams with best-in-class remote monitoring and management, enabling them to keep their clients and business safe from cybercrime, scale their business and open new revenue streams. VSA 10 reduces your software costs by being a 4-in-1 tool that combines powerful remote control, software/patch management, executive reporting and endpoint monitoring into a single, easy-to-use solution. Automate routine IT tasks, tickets and maintenance work, transforming incidence response overload into fully streamlined and efficient workflows.

SEE WHAT VSA 10 HAS TO OFFER:

DEVICE MANAGEMENT

- Windows endpoint management
- Mac endpoint management
- Linux endpoint management
- Virtual machine management
- Network monitoring
- Topology map
- Cloud endpoint monitoring
- Custom alerts and notifications
- Active Directory discovery and deployment
- Mobile device management

AUTOMATION

- Policy-based management
- Alert-based automations
- Automation deployment and scheduler
- Automated patch deployment
- Automated user onboarding
- Auto-remediation of common tickets
- Automated discovery and diagramming
- No-click user configuration hardening
- Schedule backup procedures
- Automated antivirus deployment
- Automated antimalware deployment
- Automatic detection and quarantine of ransomware
- Out-of-the-box automation scripts
- Ability to deploy automations from mobile app

PATCH MANAGEMENT

- Windows OS patching
- Windows third-party application patching
- MacOS patching
- MacOS third-party application patching
- Linux OS patching
- Server patching
- Middle-of-night patching
- Library of 230+ patchable third-party applications

REMOTE MANAGEMENT

- Best-in-class mobile application
- End-user disruption-free remote control
- Lightning-fast remote control
- Remote task manager, file xplorer and registry editor
- Copy and paste during remote control
- Remote control of network devices
- Remote control from mobile application

ENDPOINT SECURITY

- Unitrends integration
- Spanning integration
- Datto BCDR integration
- Native ransomware detection
- Secure credential transfer

TICKETING / PSA / DOCUMENTATION

- One-click integration with IT Glue
- Autotask PSA integration
- BMS PSA integration
- Vorex service desk integration
- Secure credential transfer

ADMINISTRATION

- Unitrends integration
- Spanning integration
- Datto BCDR integration
- Native ransomware detection
- Secure credential transfer

VSA 10 is the foundation of the IT Complete platform. Kaseya's IT Complete is the world's first and only purpose-built platform designed to directly address the challenges of DO-IT-ALL, multifunction, IT professionals. One vendor with everything you need, woven together to save you time, smart enough to help you get more done and in a way you can afford.

SECURE | ENDPOINT SECURITY

datto | AV

Kaseya 365

Antivirus has long been the first line of protection against cyberthreats, making it a necessity. With cyberattacks increasing exponentially year over year, it's never been more crucial for businesses to have antivirus protection in place.

NEXT-GENERATION ANTIVIRUS PROTECTION

In the current digital age, cyberthreats have evolved to a point where traditional antivirus methods may struggle to keep up. As attacks continue to rise, causing significant financial impact to businesses, it becomes clear that more advanced protection strategies are needed. Datto AV, designed with the future of cybersecurity in mind, offers an innovative and cost-effective antivirus solution. Its next-generation engine is not limited to detecting only known threats, setting it apart from conventional antivirus products. This forward-thinking approach ensures enhanced security in an increasingly complex cyber landscape.

KEY FEATURES:

NEXT-GENERATION ANTIVIRUS SECURITY ENGINE

Available today and built for tomorrow's threats, Datto AV's next-generation antivirus engine goes beyond just signature-based security.

- Leverage the strength of AI, machine learning and latest threat intelligence to identify zero-day and polymorphic malware, stopping threats before they harm your business.

- Stay ahead of evolving threats. Our cloud-based service updates multiple times a day, incorporating the latest machine learning models and heuristics.

EFFICIENCY MEETS PERFORMANCE

The endpoint user's experience is essential, and with Datto AV, you don't have to choose between performance or sophisticated protection.

- Experience top-notch security without compromising system performance. Datto AV boasts a small memory footprint, using less than 1GB of disk space.

- The internal monitoring system constantly checks performance to ensure the user is not impacted by their protection or by use of memory.

PROTECTION AND DETECTION CAPABILITIES

Datto AV scans files in real-time using its advanced unpacking capabilities to skillfully handle hundreds of runtime packers and obfuscators, plus a wide range of archive formats for thorough malware detection.

OnAccess is a real-time detection component that detects and blocks active threats on the computer. Several detection mechanics power this comprehensive component:

- On-access and on-execute of files
- On-access of relevant registry keys
- On suspicious application behavior

OnDemand is a deep search for malware on hard drives to find inactive or more complex threats. Our fast and powerful OnDemand scanning component provides the following features:

- Pre-defined fast and smart scan profiles
- Custom searches
- File, process and registry scanning
- Local and network drive scanning

DNS Filtering

- Proactively intercept malware in both HTTP and HTTPS traffic, blocking threats before they reach endpoint systems.
- Block risky sites by category (e.g., gambling, games, adult content) and prevent access to malicious domains, including command and control servers and malware hosts.
- Personalized and granular control with domain block lists, domain white-listing, and allowing specific trusted executables.

SEAMLESS INTEGRATION WITH AMSI

Integration with AMSI helps protect you from dynamic, script-based malware within supported applications — and from non-traditional cyberattacks. Protect against dynamic, script-based malware, including Microsoft Office VBA macros, PowerShell, JavaScript and VBScript.

AUTOMATIC QUARANTINE AND COMPREHENSIVE REMEDIATION

Once Datto AV quickly identifies malware and threats, it automatically quarantines the endpoint and begins remediation.

- Should the worst happen, our remediation system goes beyond detection to clean infected systems thoroughly.
- Effectively cleans infected systems by disinfecting the file system, host file, scheduled tasks and registry artifacts and removing malicious WMI event subscriptions. It addresses reinfection persistence, resets system settings and can reboot the system if needed.

INTEGRATIONS	SUPPORTED PLATFORMS	MINIMUM HARDWARE REQUIREMENTS
Datto EDR	Windows	Dual Core with 1.6 GHz
Datto RMM	Mac	2GB free RAM (4GB recommended)
RocketCyber	Coming soon: Linux	2GB free HDD (5GB recommended)
VSA X		Intel x86 32-Bit and 64-Bit dual core

datto | AV

datto | EDR

Kaseya 365

Many of today's cybercriminals can bypass traditional defenses at will. Now, more than ever, businesses need advanced endpoint threat detection and response (EDR) in addition to having an antivirus installed on each endpoint.

Unfortunately, most small and medium-sized businesses can't afford to use traditional EDR solutions, which are costly and cumbersome to deploy and manage. The same goes for managed service providers (MSPs) that may lack the resources and professional expertise required to effectively utilize traditional EDR.

This leaves businesses exposed to ransomware, credential harvesting and other types of attacks that can cost up to $8,000 per hour from the time of the known attack to remediation.

HIGHLY EFFECTIVE, YET EASY-TO-USE ENDPOINT DETECTION AND RESPONSE

Datto EDR provides effective endpoint detection and response in an affordable, easy-to-use, manage-and-deploy package. Unlike other EDR products that are built for large-scale enterprise SOC teams, Datto EDR eliminates common EDR issues, such as high cost, management complexity and alert fatigue. Each alert comes with a quick, easy-to-execute set of response guidelines to support your team in isolating infected hosts, terminating processes and collecting additional evidence.

- Sophisticated threat detection and response: Datto EDR detects suspicious behaviors and threats that evade traditional defenses so you can respond quickly, before significant damage is done.
- Click to respond: Datto EDR allows you to take action against advanced threats right from your alert dashboard. Isolate hosts, terminate processes, delete files and more without wasting precious seconds.
- Detect fileless attacks with behavioral analysis: Our patented deep memory analysis ensures you are informed of even the most elusive threat actors.
- MITRE ATT&CK mapping: Alerts are mapped to the MITRE ATT&CK framework to provide context and helpful clarity to your team, reducing the security expertise required to effectively respond.
- Smart recommendations: Our seasoned security analysts have distilled their experience into automated mitigation recommendations, so our alerting engine will help your team through the remediation process in a quick and efficient manner.
- Scalable, remote response actions: The unique click-to-respond feature supports your team in taking action against threats as quickly as they are detected to reduce potential damage.
- Deep integration: Datto EDR integrates with Datto RMM for efficient endpoint management. Also, for those who use the Kaseya IT Complete platform, Datto EDR integration eliminates the need to switch consoles for a seamless endpoint security experience.

datto | EDR

Kaseya 365

FEATURE HIGHLIGHTS

COMPLETE ENDPOINT PROTECTION

Datto EDR seamlessly integrates with Datto AV, enabling proactive, real-time endpoint protection without additional agent installation. Microsoft Windows Defender Antivirus can also be managed directly from Datto EDR. Antivirus solutions identify malware automatically based on suspicious and malicious behaviors at the endpoint, such as unusual processes, unexpected startup locations and modifications in registry keys, file system or file structure. Datto EDR enforces a secure configuration and adds monitoring capabilities, further enhancing endpoint protection.

KEY PREVENTION FEATURES:

- Block potentially unwanted applications
- Block risky DNS requests
- Quarantine threats
- Alert management inside EDR console
- Scheduled and ad hoc scans
- Manage exclusions

Datto EDR's ability to prevent threats consistently scores very high in independent testing. Used in conjunction with Datto AV, it provides top value while providing seamless integration.

DETECTION

Datto EDR detects suspicious behaviors as well as fileless malware and ransomware, automatically terminating malicious activities and isolating infected endpoints to prevent further spread of a cyberattack

KEY DETECTION FEATURES:

- Real-time endpoint security monitoring
- Deep memory monitoring and analysis
- Advanced threat detection combining static detection with behavior and anomaly-based detection
- MITRE ATT&CK mapping
- Behavioral-based update to Ransomware Detection and containment
- Modular threat-hunting capabilities
- Real-time escalation through alerts, integrations, Webhooks and email

Datto EDR's advanced real-time detection and isolation capabilities reduces time to response to the minimum. Enhanced by remote response capabilities, Datto EDR helps prevent the spread of malware within the infected organization.

THREAT INTELLIGENCE AND ANALYSIS

Backed by a threat intelligence and analyst team that constantly investigates previously unknown and suspicious malware samples, Datto EDR provides round-the-clock protection against the latest threats

KEY FEATURES:

- Integrated threat intelligence from numerous intelligence and community sources
- Malware sandbox analysis
- Analysis of cryptographic hashes of executables
- Digital forensic analysis of previously unknown and suspicious threats
- Threat enrichment and categorization service
- Advanced correlation engine

With Datto EDR, you can be sure that your endpoint security reflects the most up-to-date threat intel and forensics, reducing the risk of missing unknown threats.

RESPONSE

With Datto EDR, users can easily respond to cyber incidents as they occur, even from a remote location. Using a unique console, users are empowered to take the following response actions:

- Device isolation
- Process termination
- Execution of threat response scripts across multiple devices
- Templated threat remediation recommendations
- Quick and easy encrypted file recovery with Ransomware Rollback
- Automated Threat Response

These capabilities, together with advanced security dashboards offering a single-pane-of-glass view into all security alerts and device compliance issues, enable users to respond immediately to cyberthreats when needed.

INTEGRATIONS

- Kaseya IT Complete
- Datto RMM
- RocketCyber Managed SOC
- Integration via API
- Webhooks (SIEM, ticketing systems)
- VSA X
- Autotask
- BMS
- Datto AV

SUPPORTED PLATFORMS

- Windows
- Linux
- macOS

datto | EDR

AN INCREASING THREAT

Having the right cybersecurity tools in place is more important than ever. Year-over-year ransomware attacks have increased by 92.7%(1) with the average ransom demanded during an attack being roughly $5,600. What's worse, the downtime after an attack can cost up to 50 times more than the ransom itself[(2)].

There are countless tools that you can use to reduce downtime and protect businesses from security threats. Remote monitoring and management (RMM) platforms have always played an important role in reducing downtime and protecting businesses from security threats through real time monitoring and patching to keep managed devices secure from known vulnerabilities.

REDUCE THE RISK OF RANSOMWARE

Kaseya's RMM offerings provide a secure and full-featured cloud platform, enabling a business's IT operations team to remotely monitor, manage and support every endpoint under contract. Ransomware Detection provides an extra layer of security within the RMM solution. It monitors for crypto-ransomware on endpoints using behavioral analysis of files and alerts you when a device is infected. Once detected, the RMM solution attempts to stop the ransomware process and isolates the device to prevent the ransomware from spreading.

Ransomware Detection offers these benefits:

- **Monitor for ransomware at scale.** Ransomware Detection's powerful policy-driven approach allows you to easily monitor targeted devices and specify what the monitor looks for prior to creating an alert (e.g. locations, extensions, priority of alerts).

- Receive immediate notification when ransomware is detected. Instead of waiting for a user to report the issue, Ransomware Detection will automatically notify technicians the moment files start being encrypted by ransomware. Additionally, integrations with key tools, such as PSA, ensure the right resources can be notified and tickets created immediately.

- Prevent the spread of ransomware through network isolation. Once ransomware is detected, Ransomware Detection will attempt to kill the ransomware process and can automatically isolate the affected device from the network.

- Remediate issues remotely. Devices automatically isolated from the network still maintain contact with Ransomware Detection allowing technicians to take effective action to resolve the issue.

- Recover with continuity products. When Ransomware Detection is integrated with business continuity and disaster recovery (BCDR) products, technicians can quickly recover from the ransomware outbreak by restoring the impacted endpoint to a previous state.

2 Datto's Global State of the Channel Ransomware Report

RocketCyber

MANAGED DETECTION & RESPONSE

Kaseya 365

Managed SOC

24/7 Threat Monitoring

Eliminate modern, sophisticated cyberthreats with RocketCyber Managed SOC, the industry's most advanced security operations center.

Comprehensive managed detection and response

ENDPOINT SECURITY

Protect your endpoints with Windows and MacOS event log monitoring, advanced breach detection, malicious les and processes, threat hunting, intrusi on detection, third-party next-gen AV integrations and more.

NETWORK SECURITY

Gain new levels of network protection with rewall and edge device log monitoring integrated with real time threat reputation, DNS information and malicious connection alerts.

CLOUD SECURITY

Secure the cloud with Microsoft 365 security event log monitoring, Azure AD monitoring, Microsoft 365 malicious logins and overall Secure Score.

24/7 MANAGED DETECTION & RESPONSE POWERED BY CYBERSECURITY EXPERTS

RocketCyber is a white labeled managed SOC that detects malicious and suspicious activity across three critical attack vectors: Endpoint, Network and Cloud. Our team of cybersecurity veterans hunt, triage and work with your team when actionable threats are discovered. RocketCyber's services include:

- Continuous monitoring - Around the clock protection with real-time advanced threat detection.
- Advanced security stack - 100% purpose-built platform backed by more than 50 years of security experience, optimized to empower businesses and MSPs alike to fend o devastating cyberthreats.
- Breach detection - We catch sophisticated and advanced threats that bypass traditional AV and perimeter security solutions.
- Threat hunting - An elite cybersecurity team proactively hunts for malicious activities so you can focus on other pressing matters.
- No hardware requirements - Patent-pending cloud-based technology eliminates the need for costly and complex on-premise hardware.

RocketCyber Key Features

We save you time and money by leveraging your existing tools and cybersecurity investments across your endpoints, networks and cloud environments. This allows you to focus on what matters most — your business.

COMPREHENSIVE MONITORING

Monitor, search, alert and report on the 3 attack pillars: network, cloud and endpoint log data spanning:

- Windows, macOS & Linux security events
- Firewall & network device events
- Offivce 365 & Azure AD cloud events.

THREAT INTELLIGENCE AND HUNTING

Real-time threat intelligence monitoring, connecting to premium intel feed partners gives our customers the largest global repository of threat indicators for our SOC analysts to hunt down attackers and nd advanced threats.

BREACH DETECTION

Detect adversaries that evade traditional cyber defenses. We identify attacker tactics, techniques and procedures, aligning to MITRE ATT&CK. This allows our SOC analysts to detect indicators of compromise before any damage is done.

INTRUSION MONITORING

Real-time monitoring of malicious and suspicious activity, identifying indicators such as connections to terrorist nations, unauthorized TCP/UDP services, backdoor connections to command and control servers, lateral movements and privilege escalation.

NEXT-GENERATION MALWARE

Use your preferred malware prevention or leverage our command and control application for Microsoft Defender, backed up by our detection of malicious les, tools, processes and our automatic ransomware detection and quarantine.

PSA TICKETING

Our SOC analysts investigate each alert, triaging them to produce tickets for your PSA system, along with the remediation details so you can do more without having to hire additional staff.

Security app store

Get more by monitoring your existing tools. With our App Store, simply turn on the monitoring you want for more than 35 popular cybersecurity products, including:

- AV/AM monitoring with Datto, Bitdefender, Cylance, Deep Instinct, SentinelOne, Sophos, Webroot, Windows Defender
- Firewall Analyzer & Monitoring with Barracuda, Cisco Meraki, Fortinet, Juniper, pfSense, SonicWall, Ubiquiti, Untangle, WatchGuard
- Email and DNS Monitoring with Barracuda, DNSFilter, IRONSCALES, Microsoft 365
- ***And much more!***

ADVANCED SOFTWARE MANAGEMENT

Improve endpoint security and customer experience by ensuring all applications are fully updated with Advanced Software Management for Datto RMM and VSA 10

Security is the cornerstone of the Datto RMM and this extends to devices' applications. Advanced Software Management builds on the established Software Management framework within Datto RMM and VSA 10 to grant users access to an expanded application list to help further secure device software against online threats and vulnerabilities.

KEY FEATURES:

- Support for over a hundred additional applications within Software Management
- Ability to uninstall applications using the Software Management engine
- Policy-based approvals and deployment
- Manual approval of updates per application, site or device
- Software Management report and Dashboard widgets
- Flexible licensing
- Device-level visibility and error reporting in Compliance Manager GRC

EXPANDED APPLICATION COVERAGE

Advanced Software Management expands Datto RMM's and VSA 10's coverage to 200+ out-of-the-box third-party applications that can be updated using a Kaseya RMM solution. Some of these third-party applications include:

Audacity
Box Drive
Cisco Webex Meetings
Dropbox
Evernote
Google Drive
Jabra Direct
KeePass 2
LibreOffice
Microsoft .NET Framework
Microsoft Office 365
OpenOffice
Opera Browser
RealVNC VNC Server
Slack
TeamViewer
Tight VNC
UltraVNC
VMware Workstation Player/Pro
WinRAR
WinZip

Third-party patching is an integral part of safeguarding your business against cyberattacks and critical data loss. Advanced Software Management provides you with an expanded library, plus the capabilities to comprehensively automate updates and identify software vulnerabilities.

BACKUP | ENDPOINT BACKUP

datto
ENDPOINT BACKUP

Kaseya 365

Datto Endpoint Backup is designed for MSPs to protect their clients' Windows servers, virtual machines (VMs), cloud instances, desktops and laptops from data loss. Designed to maximize MSPs' profits, it enables recovery of entire systems and select data if downtime or cyberattacks occur.

Protect all data wherever IT lives™

Although implementing backup for every Windows endpoint is paramount for any organization, it should not break the bank for either MSPs or their clients. Now you can back up all Windows systems — in primary data centers, at remote or distributed locations, in VMs, in any cloud, in the offices or with remote employees — and leave no workload behind.

INDUSTRY-BEST MARGINS

At Datto, we set out with a vision many years ago to create a world where data loss and downtime are nonexistent and where backup is a necessity, not a luxury. Datto Endpoint Backup enables MSPs to provide reliable and cost-effective backup services for all Windows endpoints, ensuring profitability for MSPs and affordability for clients.

EVERYDAY DATA PROTECTION

Datto Endpoint Backup provides complete protection against common everyday data loss scenarios, such as ransomware, accidental deletions, hardware failure and lost or stolen devices.

RELIABLE, APPLIANCE-FREE WINDOWS BACKUP

Datto Endpoint Backup uses image-based backup technology, removing the need to procure or manage additional hardware. It provides software-only Windows backup directly to the Datto Cloud, ensuring your data is protected no matter what.

UNIFIED EXPERIENCE

Datto Endpoint Backup is managed through the familiar and proven Datto Backup Portal. This enables MSPs to manage all clients and users in one place with tools like Datto SIRIS, ALTO, Backup for Microsoft Azure, Endpoint Backup with Disaster Recovery and SaaS Protection — increasing MSP technician productivity.and SaaS Protection — increasing MSP technician productivity.

Datto Endpoint Backup

Datto Endpoint Backup is purpose-built for MSPs. It offers direct-to-cloud backup without appliances, single-pane-of-glass management, easy deployment and streamlined day-to-day operations — all delivered to multiply MSPs' operating margins. It offers replication to the secure and private Datto Cloud every two hours to protect data from downtime, cyberattacks and outages.

ENTERPRISE-GRADE PROTECTION

» A proven backup solution built on Datto SIRIS technology, delivering consistent management and protection across endpoints, servers and the cloud.

» Outstanding resilience with backup to the secure and reliable Datto Cloud ensures data protection and easy recovery.

RAPID AND RELIABLE RECOVERY

» Backups every two hours to the secure Datto Cloud enable maximum redundancy and optimal recovery time objective/ recovery point objective.

» Streamlined restore via a simple recovery process managed through a single, intuitive interface, allowing recovery of multiple files, folders or the entire disk as required.

BUILT TO SCALE FOR MSPS

» Profitability and predictability with industry-best pricing designed to maximize MSP profits.

» Single pane of glass to manage all Datto backups, organized in a client-centric view for consistent data protection across remote servers, data centers, Microsoft Azure, PCs and SaaS

.

» Built-in integration with Datto RMM and Kaseya VSA allows rapid deployment of the solution to hundreds of systems.

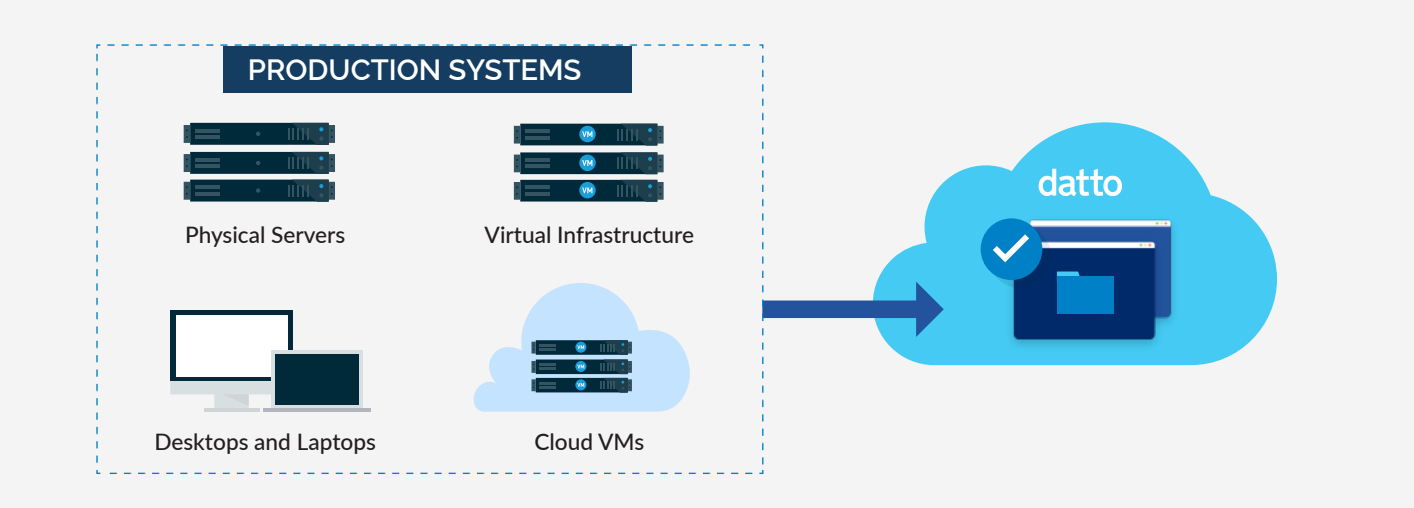
How it works

Datto Endpoint Backup backs up your clients' systems directly to the Datto Cloud every two hours.

DATTO CLOUD

The Datto Cloud is purpose-built for backup. Its immutable architecture sets the standard for a secure cloud infrastructure.

» Multiregional presence to help you support compliance regulations.
» Consistent stack for you to protect client servers, VMs, clouds and SaaS apps.



Features and system requirements

Operating systems	» Windows Server 2022 / 2019 / 2016 / 2012 R2 » Windows 11 / 10
Inverse Chain Technology™	» Send only changes to the cloud » Get independent backups » No rehydration, no synthetic backups, no recovery of chains link by link
Security options	» Forced multifactor authentication to the management portal » SSL encryption in-transit
Recovery options	» File/folder recovery » Bare metal recovery (BMR) to the same or dissimilar hardware » Export image to virtual machine format
Datto Unified Backup porta	» Shared with Datto BCDR and Datto Backup for Microsoft Azure » Monitoring of protected on-premises and cloud systems » Client-centric status page with backup progress and settings
Bandwidth throttling	» Limit internet connection usage to reduce impact on production applications
Email alerting	» Receive alerts on the status of backups
MSP stack integrations	» Mass agent deployment via Datto RMM and Kaseya VSA
Storage Capacity	» Includes 5TB of pooled storage when purchased as part of a Kaseya 365 license

Protecting business data wherever it lives

Datto Unified Backup gives MSPs the comprehensive tools necessary to protect their clients' files and applications, whether they live on local servers, SaaS applications, end-user computers or the cloud. Datto offers data protection solutions built specifically for MSPs that are reliable regardless of the size of the infrastructure. With a wide array of restore options to match different recovery scenarios, Datto Backup provides MSPs and clients peace of mind, knowing critical business data can be restored in seconds and normal business operations can continue in the event of a disaster or data loss.

AUTOMATE | ENDPOINT AUTOMATIONS

AUTOMATE

Kaseya 365 Essential 20 Automations

Kaseya 365 not only provides complete endpoint management, security and backup for one low subscription price, it also utilizes 20 essential integrations to automate workflows and significantly reduce errors.

Ticket Remediation

	AUTOMATION NAME	DESCRIPTION	IMPACT	TIME SAVED IN MINUTES (per Month)	HOME MODULE	SUPPORTING MODULE
1.	Endpoint Shortcut for EDR	Datto RMM web remote from Datto EDR hosts	Reduce the number of clicks to go from an EDR detection alert into the actual machine to verify the threat	200	Datto EDR	Datto RMM
2.	Endpoint Shortcut for AV	Datto RMM web remote from Datto AV hosts	Reduce the number of clicks to go from a Datto AV detection alert into the actual machine to verify the threat	200	Datto AV	Datto RMM

Service Delivery

	AUTOMATION NAME	DESCRIPTION	IMPACT	TIME SAVED IN MINUTES (per Month)	HOME MODULE	SUPPORTING MODULE
3.	Alert Trigger for EDR Events	Datto EDR security event collation into Datto RMM alerts	Centralize alerts into primary alerting module and consolidate events	250	Datto RMM	Datto EDR
4.	One-Deploy for RMM Policy (VSA 9)	Native VSA 9 policy for Ransomware Detection	Minimize time configuring rules of ransomware detection and response on endpoints	50	VSA 9	Ransomware Detection
5.	One-Deploy for RocketCyber	RocketCyber install and activation from Datto RMM	Protect endpoints faster and reduce deployment time for RocketCyber	10	Datto RMM	RocketCyber
6.	One-Deploy for RMM Ransomware Policy	Native Datto RMM policy for Ransomware Detection	Minimize time configuring rules of ransomware detection and response on endpoints	50	Datto RMM	Ransomware Detection

Kaseya 365 Essential 20 Automations

Customer Hygiene

	AUTOMATION NAME	DESCRIPTION	IMPACT	TIME SAVED IN MINUTES (per Month)	HOME MODULE	SUPPORTING MODULE
7.	SmartLook for EDR	Datto EDR events in Datto RMM dashboard	Minimize clicks to perform basic health checks, like ensuring security threat alerts and active agents demonstrate full coverage of a client environment	50	Datto RMM	Datto EDR
8.	True-Sync for EDR Policy	Datto EDR deployment through Native Endpoint Security Policy in Datto RMM	Protect endpoints faster and reduce deployment time for EDR	50	Datto RMM	Datto EDR
9.	True-Sync for Organizations	Datto EDR Location Sync from Datto RMM	Onboard onto EDR faster	10	Datto EDR	Datto RMM
10.	One-Deploy for Patching	Native Datto RMM policy for third-party patching	Minimize time configuring rules of patching software on endpoints during customer onboarding	10	Datto RMM	Advanced Software Management
11.	True-Sync for Health Status	Datto AV Agent Install and Health Status in Datto RMM	Minimize clicks to perform basic health checks, like ensuring AV is running on all endpoints of a client environment	10	Datto RMM	Datto AV
12.	One-Deploy for Backup Install	Endpoint Backup Install and Activation from RMM	Reduce deployment time and protect endpoints with antivirus faster	10	Datto RMM	Endpoint Backup
13.	One-Deploy for RMM 3PP Policy	Native VSA 10 RMM policy for third-party patching	Minimize time configuring rules of patching software on endpoints	10	VSA 10	Advanced Software Management
14.	One-Deploy for RMM 3PP Policy	Native VSA 9 RMM policy for third-party patching	Minimize time configuring rules of patching software on endpoints	10	VSA 9	Advanced Software Management
15.	One-Deploy for Ransomware Detection	Ransomware detection native deploy with EDR	Minimize time required to deploy ransomware detection and rollback on endpoints	50	Datto EDR	Ransomware Detection
16.	SafeCheck for EDR Activity	RocketCyber monitoring for Datto EDR	Obtain clearer insight into suspicious activities that affect an endpoint	250	RocketCyber	Datto EDR
17.	SafeCheck for AV Activity	RocketCyber monitoring for Datto AV	Obtain clearer insight into suspicious activities that affect an endpoint	250	RocketCyber	Datto AV
18.	True-Sync for Organizations	Datto EDR Location Sync from VSA 10	Onboard onto EDR faster	10	VSA 10	Datto EDR
19.	True-Sync for EDR Health Status	Unifiedendpoint security with Datto EDR and VSA 10	Minimize clicks to perform basic health checks, like ensuring EDR is running on all endpoints of an client environment	10	VSA 10	Datto EDR
20.	True-Sync for AV Health Status	Unified endpoint security with Datto AV and VSA 10	Minimize clicks to perform basic health checks, like ensuring AV is running on all endpoints of a client environment	10	VSA 10	Datto AV

Kaseya 365

COMPONENTS AND ESSENTIAL AUTOMATIONS

UNLOCK THE POTENTIAL
of Components and Essential Automations with Kaseya 365!

kaseya.com/products/kaseya-365