Datto, Inc.

SOC 3

Independent Service Auditor's Report on Management's Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security, Availability, and Confidentiality

November 1, 2022 – October 31, 2023

200 Second Avenue South, Suite 478
St. Petersburg, FL 33701

200 Second Avenue South, Suite 478
St. Petersburg, FL 33701
www.ascendaudit.com

INDEPENDENT SERVICE AUDITOR'S REPORT

The Management of Datto, Inc.
701 Brickell Avenue, Suite 400
Miami, FL 33131

Scope

We have examined Datto, Inc.'s ("Datto", or "the Company") description of controls for its Information Technology General Controls (ITGC) system and related transactions throughout the period November 1, 2022 through October 31, 2023, based on the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report *(With Revised Implementation Guidance – 2022)*(AICPA, *Description Criteria*), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period November 1, 2022 through October 31, 2023, to provide reasonable assurance that Datto's service commitments and system requirements were achieved based on the trust service criteria for security, availability, and confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)*, in AICPA *Trust Services Criteria.*

Subservice Organizations

Datto and its business units (i.e., products) utilize the following subservice organizations to provide services and application delivery:

- Bamboo HR for Human Resources information system (HRIS)
- Atlassian for source code repository, version control, and project management
- Salesforce for customer relationship management and support ticketing
- Sunguard, Noris Networks, Tierpoint, Aligned Energy, eStruxture, Equinix, Cyxtera, Aptum Technologies, CoreSite, Verne Global, NextDC, and Noris Networks for data center services
- Amazon Web Services (AWS) and Microsoft Azure for infrastructure-as-a-service and cloud computing

The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Datto, to achieve Datto's service commitments and system requirements based on the applicable trust services criterion of security, availability, and confidentiality. The description presents Datto's controls, the applicable trust services criteria of security, availability, and confidentiality and the types of complementary subservice organization controls assumed in the design of Datto's controls. The description does not disclose the actual controls at the subservice organizations.

Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls. Our examination did not extend to controls at the service organizations listed.

Datto, Inc.'s Responsibilities

Datto is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Datto's service commitments and system requirements were achieved. In Section II, Datto has provided its assertion titled "Assertion of Datto, Inc. Service

Organization Management" about the description and the suitability of design and operating effectiveness of controls stated therein. Datto is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Ascend Audit & Advisory's Responsibilities

Our responsibility is to express an opinion on the description of the suitability of the design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs. There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with policies or procedures may deteriorate.

Opinion

In our opinion, Datto's controls over the system were effective throughout the period November 1, 2022 through October 31, 2023, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period.

Ascend Audit & Advisory

St. Petersburg, FL

December 19, 2023

ASSERTION OF DATTO, INC. SERVICE ORGANIZATION MANAGEMENT

We have prepared the description of Datto, Inc.'s Information Technology General Controls system ("system" or "the system") throughout the period November 1, 2022 through October 31, 2023, ("the description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization System in a SOC 2 Report (With Revised Implementation Guidance – 2022)*(AICPA, *Description Criteria*). The description is intended to provide report users with information about the system that may be useful when assessing the risks arising from interactions with Datto Service Organization's system, particularly information about system controls that Datto has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)*(AICPA *Trust Services Criteria*).

Datto and its business units (i.e., products) utilize the following subservice organizations to provide services and application delivery:

- Bamboo HR for Human Resources information system (HRIS)
- Atlassian for source code repository, version control, and project management
- Salesforce for customer relationship management and support ticketing
- Sunguard, Noris Networks, Tierpoint, Aligned Energy, eStruxture, Equinix, Cyxtera, Aptum Technologies, CoreSite, Verne Global, NextDC, and Noris Networks for data center services
- Amazon Web Services (AWS) and Microsoft Azure for infrastructure-as-a-service and cloud computing

The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Datto, to achieve Datto's service commitments and system requirements based on the applicable trust services criterion of security, availability, and confidentiality. The description presents Datto's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Datto's controls. The description does not disclose the actual controls at the subservice organizations. The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Datto, to achieve Datto's service commitments and system requirements based on the applicable trust services criteria. The description presents Datto's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Datto's controls.

We confirm, to the best of our knowledge and belief, that:

a. The description presents Datto's system that was designed and implemented throughout the period of November 1, 2022 to October 31, 2023, in accordance with the description criteria.

   i. The description contains the following information:

      (1) The types of services provided.

      (2) The components of the system used to provide the services, which are the following:

      - *Infrastructure* – The physical and hardware components of a system (facilities, equipment, and networks).
      - *Software* – The programs and operating software of a system (systems, applications, and utilities).
      - *People* – The personnel involved in the operation and use of a system (developers, operators, users, and managers).
      - *Procedures* – The automated and manual procedures involved in the operation of a system.

- *Data* – The information used and supported by a system (transaction streams, files, databases, and tables).

(3) The boundaries or aspects of the system covered by the description.

(4) How the system captures and addresses significant events and conditions.

(5) The process used to prepare and deliver reports and other information to user entities and other parties.

(6) If information is provided to, or received from, subservice organizations or other parties, how such information is provided or received; the role of the subservice organization and other parties; and the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

(7) For each category being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the Company's system.

(8) For subservice organizations presented using the carve-out method, the nature of the services provided by the subservice organization; each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the Company, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria; and for privacy, the types of activities that the subservice organization would need to perform to comply with privacy commitments.

(9) Any applicable trust services criteria that are not addressed by a control at the Company or a subservice organization and the reasons, therefore.

(10) Other aspects of the Company's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.

(11) Relevant details of changes to the Company's system during the period covered by the description.

ii. The description does not omit or distort information relevant to the Company's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

b. The controls stated in the description were suitably designed throughout the period November 1, 2022 to October 31, 2023, to provide reasonable assurance that Datto's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Datto's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period November 1, 2022 to October 31, 2023, to provide reasonable assurance that Datto's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Datto's controls operated effectively throughout that period.

DESCRIPTION OF DATTO, INC.'S INFORMATION TECHNOLOGY GENERAL CONTROLS SYSTEM

Company Overview

Datto, now a Kaseya company, is a leading global provider of security and cloud based software solutions purpose-built for Managed Service Providers (MSPs), Datto believes there is no limit to what small and medium businesses (SMBs) can achieve with the right technology. Datto's proven Unified Continuity, Networking, Endpoint Management, and Business Management solutions drive cyber resilience, efficiency, and growth for MSPs. Delivered via an integrated platform, Datto's solutions like Datto Azure DCMA, BCDR, BitDam, Cloud Continuity for PC, Datto Commerce, EDR, Networking, RMM, SaaS Protection, Workplace, and PSA Autotask help its global ecosystem of MSP partners serve over one million businesses around the world. From proactive dynamic detection and prevention to fast, flexible recovery from cyber incidents, Datto's solutions defend against costly downtime and data loss in servers, virtual machines, cloud applications, or anywhere data resides. Datto has won awards for its rapid growth, product excellence, superior technical support, and for fostering an outstanding workplace. Datto's corporate headquarters is in Miami, FL, with offices in North America, EMEA, and APAC regions.

Products and Services Overview

Autotask PSA

Datto's cloud-based IT business management tool, Autotask PSA, is a robust IT Business Management solution that combines service desk, contracts, SLAs, projects, CRM, time, and billing. The Autotask PSA platform allows technology providers to provide better, more efficient service at peak profitability – and gives them a real-time view of critical business information on a single pane of glass. Autotask PSA tool provides the following features:

- CRM (Customer Relationship Management)
- Ticketing
- Project Management
- Invoicing
- Reporting

Backupify (SaaS Protection)

Datto's Backupify/SaaS Protection application is a cloud-based backup and recovery solution for application data including Google Apps, and Office 365. Through the report, the SaaS Protection products and services may be referred to as "SaaS Protection" and/or "Backupify." "Backupify" is an alternate trade name that Datto uses for the SaaS Protection product and services. SaaS Protection solution include the following services:

- Automated Continuous Backup
- Flexible Retention
- Admin Audit Log
- Ransomware Protection
- Recover Quickly
- Easy Export

As more services and organizations migrate from local hard drives to the always-on cloud, SaaS Protection is pioneering the protections and processes that will keep clients' irreplaceable online information safe, available, and under their control. The SaaS Protection service is an easy-to-use solution that enables data backups from multiple SaaS platforms through a single user interface; backups run on demand or on a customer-defined schedule. Backup data is maintained on the Datto Cloud platform, separate from customers' SaaS providers' repositories.

BCDR

Datto's Business Continuity & Disaster Recovery (BCDR) solution has been used by companies nationwide. Datto's cloud-based storage and data recovery services and their related controls are key differentiators in providing and maintaining a secure cloud-based storage and recovery solution to its customers. The solution consists of a hybrid cloud backup solution, which indicates a local appliance that takes backups of a protected machine and a set of replicated cloud backups, stored in the Datto Cloud, providing MSP's and their clients with:

- Ransomware Protection
- Fast Recovery

BitDam

BitDam is a SaaS platform making enterprise communications safe to click. BitDam cyber security solutions protect enterprise communications from advanced content-borne threats. BitDam's mission is preventing cyber-attacks on hardware and logical exploits, N-Day, and Zero-Day attacks from within the communication stream.

Cloud Continuity

Datto's Cloud Continuity (CC) solution has been used by companies nationwide. Datto's cloud-based storage and data recovery services and their related controls are key differentiators in providing and maintaining a secure cloud-based storage and recovery solution to its customers.

Cloud continuity has numerous features to help users easily and securely store and access their data.

- Streamline Recovery – easily restore individual files and folders, rollback from ransomware, or restore the entire PC image to a new device.

- Screenshot Verification – ensure backups are verified for reliable recovery with integrity checks that validate every backup and provide an alert if there are issues.

- RMM Integration – save time and perform mass deployments easily and efficiently by utilizing RMM alongside Cloud Continuity.

DWP

Datto's Workplace Cloud System, formally known as DWP, offers the following important benefits to its business customers:

- Mobile Collaboration – Flexible access to the most up-to-the-minute business content empowers employees to make better and more informed decisions to help drive the business forward faster. Datto Workplace facilitates optimized content delivery and rendering of any type of business content from users' mobile devices. The Datto Workplace One-App concept and team-based sharing helps ensure that corporate content stays in the right hands.

- Enterprise-Grade Security – Critical business content needs to be secured. Policy-based control of content, seats, and devices is paramount to maintain corporate security. Datto Workplace is an enterprise-grade service with stringent levels of security. With geo-redundant data centers in the U.S., EU, Canada, and Australia, Datto adheres to local regulations for data in all major regions of the world.

- Purpose-Built for Business and Users – Datto Workplace is flexible and open, designed for the specific needs of IT departments in larger companies where control and management of cloud services is critical to business operations. With policy-based control of content, seats, and devices, providing secure access for employees and partners to work together on projects with the proper controls is a top priority.

RMM

Datto RMM is a cloud based remote monitoring and management platform that enables customers to administer their clients efficiently and effectively at scale. The scope of this audit is to review the Security and Availability Trust Services Principles for the Datto RMM service offering. While the vast majority of the service components making up regional clouds are identical, the focus of this audit will be centered on the services and systems supporting the U.S. (United States) and Canada Datto RMM environment.

Partners and end users deploy a software agent to machines they wish to protect and manage through the platform. These agents communicate back to the RMM cloud data center, where services enable remote access, performance monitoring, software management, and a long list of other functionalities once the agent is enrolled. RMM solution include the following:

- Flexible, Automated Patch Management
- Automation and Scripting
- Real-Time Monitoring
- Network Topology Mapping
- Ransomware Detection

Datto Networking

Datto Networking enables MSPs to efficiently deploy a suite of comprehensive managed networking services. Fully managed in the cloud, Datto Networking simplifies network deployments with smarter devices, always connected networking and fully integrated failover enabling MSPs to cost effectively support at a competitive recurring revenue price point. Key offerings including the following:

- Network Appliance
- Networking Switches
- Networking Wi-Fi

Azure Protect

Datto's cloud based storage and data recovery services and their related controls are key differentiators in providing and maintaining a secure cloud-based storage and recovery solution to its customers. Datto Continuity for Microsoft Azure has numerous features to help users easily and securely store and access their data.

Datto Commerce (Kaseya Quote Manager)

The solution automates the processes of product selection, quoting, and sales of IT products and services for MSP clients. Its SaaS platform includes an efficient selling or quoting feature and a simple user interface to streamline sales, resulting in significant time savings and efficiency for MSPs. The well-designed UX creates easy-to-edit proposals for MSPs in minutes or less. The simplified UI (User Interface) makes product search simple for SMB (Server Message Block) clients to receive access, shop, and purchase from approved devices catalogued by MSPs, improving the customer experience.

System Description

Service Commitment and System Requirements

Datto's security, availability, and confidentiality commitments to customers are documented and communicated to customers in the Kaseya Master Services Agreement and the description of service documents published on the customer facing Website. The principal security, availability, and confidentiality commitments include, but are not limited to:

- Maintain appropriate administrative, physical, and technical safeguards to protect the security and availability of the Datto Products platform and the customer data in accordance with Datto's security requirements.
- Perform annual third-party security and compliance audits of the environment, including, but not limited to:
    - Reporting on Service Organization Controls (SOC) relevant to security, availability, and confidentiality
- Use formal HR (Human Resources) processes, including background checks, code of conduct and company policy acknowledgements, security awareness training, disciplinary processes, and annual performance reviews.
- Access management procedures for the request, approval, provisioning, review, and revocation of Datto personnel with access to any production systems.
- Prevent malware from being introduced to production systems.
- Monitor the production environment for vulnerabilities and malicious traffic.
- Use industry standard secure encryption methods to protect customer data at rest and in transit.
- Transmit unique login credentials and customer data via encrypted connections.
- Maintain a disaster recovery and business continuity plan to ensure availability of information following an interruption or failure of critical business processes.
- Maintain and adhere to a formal incident management process, including security incident escalation procedures.
- Maintain confidentiality of customer data and notify customers in the event of a data breach.
- Identify, classify, and properly dispose of confidential data when retention period is reached and/or upon notification of customer account cancellation.

Datto regularly reviews the security, availability, and confidentiality performance metrics to ensure these commitments are met.

Components of the System

Datto's control environment (the "System") is comprised of the following components:

- Infrastructure (work from home locations, workstations, and cloud hosting)
- Software (cloud-based solutions and applications)
- People (employees, consultants, and users)
- Policies and Procedures (manual and automated)
- Data (transaction streams, files, databases and tables)

The Company's environment and platform are designed and managed with security, availability, and confidentiality in mind. The following sections provide a brief description of the five components comprising the System.

Infrastructure

<u>AUTOTASK PSA Infrastructure</u>

Autotask PSA operates on three resilient, high-availability data centers. These platforms exist in regions to provide increased performance for customers around the globe. At present the core platforms are hosted in the U.S., Germany,

and the UK (United Kingdom). All communication that needs to travel between regions is performed via secure SSH (Secure Shell) Tunnels or HTTPS connections. To help to achieve the required levels of resilience and scalability, Autotask PSA infrastructure is separated into multiple logical customers facing zones.

The Production Server side in the Company's Data Center consists of:

- Load Balancing
- Server instances
- File Storage
- Firewalls

Azure Protect Infrastructure

The backbone infrastructure of the Datto Continuity for Microsoft Azure service utilizes Azure virtual cloud devices alongside a Hyper V node for restorations. Backup data is replicated to a physically separate storage system in the Datto cloud. This replication provides additional levels of data protection and durability to assure data availability in the face of a disaster.

End user and partner visibility to stored backup data in the Datto cloud is provided through the Partner Portal which offers status, management, and restoration service capabilities. The Datto Continuity for Microsoft Azure service is additionally supported by several other infrastructures, services, and application components.

Backupify Infrastructure

The backbone infrastructure for the SaaS Protection solution is a fleet of systems providing computing power and dense storage capability. These systems receive and store backup data directly from the cloud SaaS services and allow customer administrators to restore data in the cloud services event of a disaster, export the data, and backup current data at periodic intervals.

Depending on end user service levels and customer location, data might be backed up to object storage systems in the Datto data centers or AWS (S3 service). The backed-up data is also replicated within the Datto cloud for disaster recovery scenarios.

User registration and partner visibility of backed up data is also provided through the SaaS store and Partner Portal in addition to the SaaS Protection web application. Individual users/customers that are not partner managed can register to the application using the Backupify web application.

SaaS Protection 2.0 is written primarily in PHP (Symfony framework) and Scala (Akka framework) and has the infrastructure hosted in the Datto data center. The backbone infrastructure for the Backupify 2.0 solution is a fleet of storage nodes providing computing power and dense storage capability. These systems receive and store backup data directly from the cloud SaaS services and allow customer administrators to restore data in the cloud services event of a disaster, export the data, and backup current data at periodic intervals.

SaaS Protection 3.0/BTF uses similar frameworks and technologies as SaaS Protection 2.0, but rather than utilizing ZFS storage nodes for the underlying computing power, SaaS Protection 3.0/BFT uses application nodes providing computer power with a Swift cluster providing data storage. SaaS Protection 3.0/BTF also uses pod architecture.

BCDR Infrastructure

The backbone infrastructure of the Datto Cloud BCDR service is a fleet of systems providing computing power and dense storage capability. These systems receive and store backup data directly from BCDR appliances and allow end users to restore files, entire systems, or virtualize their infrastructure in the event of a disaster. Depending on end user service

levels and subscriptions, backup data may be replicated to a physically separate storage system. In geographical areas with heavy product utilization, such as the U.S., Canada and Europe, this replication occurs between systems in distinct colocation facilities. In other locations with a growing deployment base this replication occurs between systems resident in the same colocation facility. This replication provides additional levels of data protection and durability needed by end users to assure data availability in the face of a disaster.

End user and partner visibility to stored backup data in the Datto Cloud is provided through the Partner Portal which offers status, management, and restoration service capabilities. Employee visibility into systems and services is provided through the Admin Portal which offers additional status, management, and restoration capabilities that are limited to authorized employees.

The Datto BCDR service is additionally supported by a number of other infrastructure, service, and application components.

BitDam Infrastructure

Hosted in data centers in Azure which comprise multiple availability zones, the production environment includes multiple Azure cloud components such as Azure Kubernetes Services instances, Load Balancers, MySQL DBs, Storage Accounts resources, and more. The Company also uses multiple database technologies such as relational database systems, NoSQL, and in-memory databases. Databases are redundant within the production environment. These services are designed to make web-scale computing easier for BitDam.

Bit Dam's production network encompasses numerous components, including segmented internal networks, and security and monitoring tools and services responsible for redundancy and scaling. The production network is built on several tiers, where each type of server has its own segment and access rules. The infrastructure consists of synchronization components which can be scaled up when needed. The network is monitored using Azure Monitoring Services. Administrative access to the Azure portal management interface is restricted to authorized personnel.

BitDam servers run up-to-date Linux distributions which execute various programming languages and frameworks. Traffic is distributed equally, using load balancer technology, between all application servers to achieve maximum scalability. The database processing environment is based on relational database management. System applications are monitored by a centralized log management system. Servers and services are monitored by a dedicated tool and using infrastructure alerts defined on Azure. Administrative access to the Azure portal management interface is restricted to authorized personnel.

Cloud Continuity Infrastructure

The backbone infrastructure of the Datto Cloud Continuity service is a fleet of systems providing computing power and dense storage capabilities. These systems receive and store backup data directly from Cloud Continuity agents that are installed on various individual systems such as laptops or personal computers. The infrastructure allows end users to restore files or entire systems via a Recovery Launchpad on their 'Partner Portal.' Backup data is replicated to a physically separate storage system. This replication provides additional levels of data projection and durability needed by end users to assure data availability in the face of a disaster.

End user and partner visibility to stored backup data in the Datto cloud is provided through the Partner Portal which offers status, management, and restoration service capabilities. Employee visibility into systems and services is provided through the Admin Portal which offers additional status, management, and restoration capabilities that are limited to authorized employees.

The Datto Cloud Continuity service is additionally supported by several other infrastructures, services, and application components.

DWP Infrastructure

The overall Datto Workplace infrastructure consists of multiple and geo-redundant data centers (composed of modules called data center cells), and Datto components installed on users' computers where users' files reside and, optionally, on users' mobile devices such as smartphones and tablets.

This architecture has proven to be highly modular and scalable from a storage and capacity perspective and fully automated from a control and management perspective. Due to this modularity, Datto can add significant new data center capacity in less than a few weeks, which is required for scalability and agility in a rapidly evolving SaaS business model. As a result, Datto has been able to employ a near-real-time systems development methodology that supports business objectives and customer requirements that drive all aspects of scaling and managing Datto's Network Operations and IT systems.

All locations are carrier grade data center hosting facilities that are operated by their respective owners. These facilities are audited by independent service auditors for SOC 2, CSAE 3416, and ISAE 3402 controls for operating effectiveness as required. Each facility houses servers for dozens of major telecommunications, media, technology, entertainment, and financial services.

Data Center Cells

The fundamental component of the Datto Workplace architecture is the data center cell. Several data center cells are operated simultaneously and internal replication of data from cell to cell protects against failure of any one cell. Each cell consists of the following server components:

- Management Server. The Management server is the main management component in the cell and handles several key functions:
    - Secure login access
    - PXE boot images and server configurations
    - Internal DNS server
    - SMTP gateway
- Kaseya has several monitoring systems in place that keep servers running in the Datto data centers.
- Load Balance Servers are used in the environment.
- Application Servers. The application servers are where the Datto application software runs. Each application server is capable of handling Desktop Agent connections, as well as Web and mobile HTTPS sessions.
- Metadata Server. The Metadata Server stores the metadata about all the objects that each Datto user has stored in the system.
- Storage Servers. Datto has several storage solutions in place based on the product needs.

RMM Infrastructure

Datto RMM operates on multiple resilient, high availability, scaling platforms hosted within Amazon Web Services (AWS). These Platforms exist and span a number of different AWS Regions to provide increased performance for customers around the globe. At present the core platforms are hosted in the EU-WEST-1 (Ireland), US-WEST-2 (Oregon), US-EAST-1 (Virginia) and AP-SOUTHEAST-2 (Sydney) regions, with additional servers in AP-SOUTHEAST-1. All communication that needs to travel between AWS Regions is performed via Secure VPC (Virtual Private Cloud) Peering Connections or HTTPS connections. To help to achieve the required levels of resilience and scalability, Datto RMM platforms are organized using a number of different services and concepts.

RMM Applications/Services

Including but not limited to the Web Portal, Control Channel, Web Service, and Monitor Service, these services and applications provide the bulk of the logic and processing associated with the platform itself. All are deployed either to EC2 Instances via OpsWorks or as Docker containers using ECS.

Availability Zones

Within each AWS Region there exist two or more Availability Zones. These zones are distinct locations within a region that are engineered to be isolated from failures in each other, while still providing high performance, low latency inter-AZ connectivity. By hosting across multiple Availability Zones, Datto RMM is able to ensure that a failure in a single Data Center does not affect the availability of a platform.

Load Balancing

All of the core platform services (Web Portal, CC, WS, Monitor Service, etc.) within Datto RMM exist as multiple servers within AWS and are themselves only accessible through dedicated Load Balancers. For the Web Portal, this load balancing is provided via the use of the Amazon Elastic Load Balancer service, whilst the CC and WS servers use dedicated Load Balancing instances. By spreading these load balancers across multiple availability zones and using DNS Round-Robin, Datto RMM is able to ensure high availability, scalability, and performance of the platform. Servers can be commissioned and decommissioned as required with no impact to the service itself.

Server Instances

Datto RMM uses Ubuntu for the base operating system of the server instances, hosted within AWS Elastic Compute Cloud (EC2). The version used has been specifically prepared and hardened for use in AWS by Canonical Ltd, the provider of the Ubuntu platform. Server instances are launched from prebuilt and tested machine images to ensure 100% consistency. These machine images are backed up to the AWS Simple Storage Service (S3) which has 99.999999999% (11 9's) durability according to AWS. Servers are stateless in that they do not store any persistent data allowing them to be replaced on demand, negating the need for individual server backups, and ensuring that the failure of a server does not result in a loss of customer data.

File Storage

All components uploaded to the Datto RMM platform are uploaded to buckets within S3. This ensures durability of data, and also provides a highly available mechanism to securely serve these files back to devices across the globe as required. By using S3, Datto RMM ensures that components can be instantly provisioned to any number of devices over a high bandwidth connection, not tied to a static number of background instances. Access to S3 is restricted based on application requirements, with individual services only having access to the buckets and access methods (read/write/list/etc.) they require.

Firewalls

AWS EC2 instances are, by default, closed for ingress via the use of configurable security groups. By default, Datto RMM core servers are only accessible via dedicated Load Balancer or SSH Tunnel instances, which exist in separate security groups. This means that access to these instances is either via 443 for HTTPS or secure TCP traffic from Load Balancers, or via SSH Tunnel on port twenty-two through a dedicated SSH Instance. Any servers which do not require external connections are therefore locked down and accessible only on port twenty-two via first connecting to a limited access VPN (Virtual Private Networks). This security group concept extends to

Amazon's Relational Database Service (RDS) and means that the Databases that back the platforms are not externally accessible, and instead only open to connections from specific security groups.

Auto Scaling

In times of high load, Datto RMM servers can auto scale, adding additional server resources automatically to areas of the system that are most heavily utilized. Additional servers can be automatically brought online and added to the load balancer as required. Conversely, auto scaling can remove excess processing in times of minimal load. Additional server instances can be provisioned in under 60 seconds and ensure a consistent level of service for users despite platform load.

Platform Infrastructure Security

Datto RMM runs on a hardened Ubuntu Linux platform, with all instances launched from a patched and maintained Elastic Block Storage (EBS) image, based on an original provided by Canonical Ltd. Most instances exist for a maximum of one release cycle before being terminated and replaced by a newly instantiated server. This ensures consistency across all servers in the Datto RMM platform and provides a base level of security, availability, and confidentiality without the need to worry about missing critical patches or configuration for each server.

AWS Console Access

Each Datto RMM Platform is hosted within a separate AWS Account. Administration of the services provided by AWS (EC2, RDS, S3, etc.) is performed through the use of both the AWS Console and the AWS API Services for programmatic access.

Only essential staff within Datto RMM has access to these services, with access configured on a per platform basis through the use of AWS Identity and Access Management. All logins to the console are required to have a secure password in addition to the use of hardware tokens. Programmatic access to the AWS API is controlled through Secure Keys and Secrets issued via the IAM (Identity Access Management) interface.

Each user, and by extension each Secure Access Key, has their rights and permissions tailored to their role or intended usage. This ensures that should a single access key be compromised, its access is restricted to specific areas of functionality, it cannot be used to “mint” more access keys, and it can be easily revoked and replaced.

Agent

An essential component of Datto RMM cloud system, the desktop agent, is a small client application that allows for the remote management of the endpoint. The agent is used to keep the endpoint continuously connected to the cloud system for management functions. The desktop agent authenticates itself with secret keys that allows for association with the proper RMM account. 256-bit SSL (Secure Sockets Layer) is used for all communications to the cloud services. The desktop agent communicates using a proprietary method, further ensuring that information is not accessible to outside systems.

Datto Networking Infrastructure

Datto Networking is written in C, and C++. It has infrastructure hosted partly in AWS and the Datto Data Center. The backbone infrastructure for the Datto Networking solution is a fleet of systems providing computing power and storage capabilities for networking device configurations. These systems allow for the distributed configuration of networking device configurations. These systems allow for the distributed configuration of networking devices via remote management and monitoring. Configurations are configured via the web application or mobile application hosted in the

data center and then push down to the networking appliances by the check-in process. The configurations are encrypted in transit utilizing TLS (Transport Layer Security).

Datto Networking is an MSP-centric networking product line and provides the MSPs and small to medium sized businesses with the optimal blend of reliability and performance, ease of use and efficiency.

Software

Software practices common to multiple products include:

The development, testing, and migration of application changes to production systems are according to change control processes. Application development is based on NIST (National Institute of Standards and Technology) guidelines. Formalized procedures guide code development and testing. Additional staging and test systems can be brought online in a separate cloud platform. No development and test environments interact with the production environment. Developers and employees with production code deployment duties are separate.

Datto has deployed a variety of solutions and tools to minimize security vulnerabilities associated with code development and code evaluation prior to deployment to the production environment. Access to source code is restricted through the configuration of the Company's Active Directory security groups and source code repository and version control software; Datto performs a routine audit of source code repository and version control software users to validate the appropriateness of access to the system.

Datto has formalized policies and procedures that define requirements for managing application changes. The process consists of request, planning, evaluation, documentation, notification, implementation, and resolution.

Datto hosts multiple QA & staging environments in every product, that developers have access to while developing software. They test their changes there, on systems that have no relationships to production. When necessary, additional staging and test systems are brought online in a separate cloud environment. Changes selected for a release are also regression tested by the Quality Assurance team. The development and test environments do not interact with production. SaaS Protection software engineers are responsible for application development, bug fixes, code reviews, developing units test, and some automated/manual testing. Quality engineers are responsible for test framework development, test automation (API, regression, UI), as well as analysing and managing quality risk for the system.

Software practices associated with specific products include:

<u>AUTOTASK PSA Software</u>

Autotask PSA uses Windows Server for the base operating system of the server instances. The version used has been specifically prepared, templated, and hardened using CIS (Center for Internet Security) benchmark standards, to provide uniformity and consistency amongst the servers. Servers are layered and perform specific functions within the overall system, this includes web server, sessions state, and SQL server functional tiers.

- Windows Server 2019 - Application, web, and service servers
- SQL Server 2017 - Database storage for customer and data warehouse servers
- Azure DevOps Server (Team Foundation Server) - On premise code repository and version control

<u>Azure Protect Software</u>

All Datto cloud nodes are running Ubuntu 20.04. The primary technology stacks being utilized are PHP, Symfony, JavaScript, Python, Apache2, NGINX, ZFS, KVM/QEMU, Bash, and C++. The application being used to sync data between nodes, Speedsync, is developed in-house by Datto Engineering.

BCDR Software

Datto maintains an inventory of open source and SaaS software that are used to support the BCDR solution and business services.

Cloud Continuity Software

All cloud nodes are running Ubuntu 20.04. The primary technology stacks being utilized are PHP, Symfony, JavaScript, Python, Apache2, NGINX, ZFS, KVM/QEMU, Bash, and C++. Applications being used such as Speedsync, Snapctl, and the Cloud Continuity agent were developed in-house by Datto Engineering. Datto also utilizes an endpoint protection system in Cloud Continuity nodes which combines prevention and detection into a single autonomous system.

DWP Software

The Datto Workplace architecture includes two components installed on users' equipment physically separate from the Datto data center which include the Desktop Agent (in the form of a downloadable installer file for Windows, and Mac computers), and the Mobile Client (in the form of a mobile application from respective application stores for iOS and Android).

Desktop Agent Software

An essential component of Datto's Workplace Cloud System, the Desktop Agent, is a small client application that is installed on users' desktop and laptop computers. Users are required to read and accept the Datto End User License Agreement (EULA) document that covers security and availability obligations before the application will install. The Desktop Agent is used to keep the files in the system updated at all times. The Desktop Agent establishes a secure connection to Datto's Workplace Cloud System and is responsible for transferring selected information from the users' computer to Datto's Workplace Cloud System for persistent mobile access. The Desktop Agent authenticates itself with the user ID and secret keys for the proper Datto account. The Desktop Agent includes several advanced security features.

TLS or Transport Layer Security is used for all communications to the service. The Desktop Agent and Datto Workplace servers communicate using proprietary methods, further ensuring that information is unintelligible to outside systems. The Desktop Agent interacts only with the Datto servers, making it difficult to redirect information. Users can also choose what types of data can be accessed remotely, including files, folders, and email messages. Any information outside explicitly shared content is excluded.

Mobile Client Software

The Mobile Client is an optional application that can be installed on mobile devices. The Datto Workplace Mobile Client allows the exchange of data from the handset to the system and back to the users' desktop computer. Similar to the Desktop Agent, the Mobile Client establishes a secure connection to Datto's Workplace Cloud System and is responsible for transferring selected information from the users' smartphone or tablet to Datto's Workplace Cloud System for persistent mobile access. The Mobile Client authenticates itself with the user ID and secret keys for the proper Datto account. The Mobile Client also includes the same type of advanced security features as the Desktop Agent.

RMM Software

Datto's RMM source code is stored in privately hosted source code repository and version control software. Access to repository and version control is managed within AWS, requires private network access, and have security group access controls lists applied to the infrastructure. Additionally, user accounts are available only for the RMM team.

All development occurs locally on the engineer's workstation. The test environment exists within AWS and is an exact clone of the production environment, less any production customer data. Additional staging and test systems are brought online in a completely separate cloud environment as the code progresses towards deployment. The development and test environments do not interact with production.

Datto RMM DevOps engineers are responsible for application development, bug fixes, code reviews, developing units test, and some automated/manual testing. Quality engineers are responsible for test framework development, test automation (API, regression, UI), as well as analysing and managing quality risk for the system.

People

This section outlines the roles and functions of various departments crucial to security and overall compliance.

- Executive Management
- Human Resources
- IT Support
- Information Security Management
- Software Engineering
- Marketing
- Finance
- Technology

Corporate Policies and Procedures

Datto has formalized policies and procedures which are as follows:

- Asset Management Procedures
- Business Continuity and Disaster Recovery Plan
- Change Management Policy
- Code of Conduct
- Confidentiality Agreement
- Electronic Data Destruction Policy
- Employee Handbook
- Enterprise Encryption Guidelines in Information Security Policy
- Hiring and Termination Checklist
- Incident Response Plan
- Information Security Policy
- Offboarding Process
- Onboarding Process
- Patch Management Procedures
- Vendor Risk Management Policy
- Vulnerability Disclosure Policy
- Backup & Restore Policy and Procedure
- Kaseya Disaster Recovery Plan
- Data Classification Matrix & Handling Guide
- Laptop Security Policy
- Acceptable Use Policy
- Environmental Protection Policy
- Password Policy
- BYOD (Bring Your Own Device) Policy

- Physical Access Security Policy
- Records Retention Policy
- Software Development Life Cycle Policy
- Vendor Management Program
- Corporate IT MFA (Multi Factor Authentication) Admin Policy
- Work-From-Home Resource Center

Data

Data management common to multiple products includes:

Datto stores several types of customer and company data in the cloud solution platform. Sensitive data is protected through secure encryption methodologies.

Datto retains confidential information to meet legal and regulatory requirements and confidentiality commitments. Requirements for data retention are specified contractually via the customer-specific Datto Terms and Privacy Policy.

Sensitive data is secured any time it must be transmitted or received via open, public networks. All connectivity to the Datto Cloud utilizes OpenSSH with AES-256-bit encryption to protect backed-up data in transit.

Encryption practices protect information involved in the Datto Continuity for Microsoft Azure solution from incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication, and replay.

Data management associated with specific products include:

<u>AUTOTASK PSA Data</u>

- The Autotask PSA platform stores data with security and protection. For sensitive information stored in protected UDF fields, data is encrypted using chained encryption keys that are stored in various parts of the infrastructure to hinder internal collusion of key material handling.
- Where new platforms are added in the future, the location of the corresponding data center will be announced to allow customers to make appropriate decisions when reviewing concerns such as the Data Protection Directive.

<u>BitDam Data</u>

BitDam has implemented an access recertification process to monitor that only authorized personnel will have access to the systems. Accordingly, permissions to the different environments (servers, database, and application) are reviewed and approved by BitDam Management on an annual basis.

<u>DWP Data</u>

User data (customer information) means information that is stored and managed by Datto's services and includes backed-up or synced files, personal identifiable information, and any related metadata. Datto's security begins with the design of the system and flows through to the physical security of the data center and the protection of users' personal data. These protections include:

- SSL (128/168-bit or 256-bit AES depending on the capabilities of the host environment) encryption of all data transmissions.
- Proprietary communications protocols to discourage hacking.

- A modular data center design to provide ease of scalability, redundancy, and protection of data.
- Data centers that are hosted in SOC (System and Organisation Controls), ISAE 3402, and/or CSAE 3416 audited facilities.
- Encryption of files at rest on the servers using 256-bit AES with dynamic key injection and rotation.
- HTTPS based on VeriSign certificates.
- Virus scanning of all files transmitted through the system.
- Role-based access and user authentication.
- Device security (no persistent data, cookie management).

RMM Data

User data (customer information) means information that is stored and managed by Datto's services and includes backed-up or synced files, personal identifiable information, and any related metadata. Datto's security begins with the design of the system and flows through to the physical security of the data center and the protection of users' personal data. These protections include:

- Hosted in SOC 1/ISAE 3402, SOC 2, SOC 3, ISO 9001, ISO 27001, ISO 27017, or ISO 27018 audited facilities.
- A modular data center design to provide ease of scalability, redundancy, and protection of data.
- Role-based access and user authentication.
- Datto RMM is underpinned by a high availability, RDS Aurora for MySQL, RDS Aurora for PostgreSQL, DynamoDB, and Elasticsearch
- Databases are distributed across at least two availability zones in a Writer/Read-Replica or cluster arrangement.
- In the unlikely event of a database failure, Datto RMM will automatically fail over to the read-replica database in the other availability zone within a matter of minutes.
- RDS automatically patches the database software and backs up the database, storing the backups for a user-defined retention period and enabling point-in-time recovery.
- For sensitive information, in addition to access controls and platform penetration testing, this also includes encryption using AES/CBC/PKCS5Padding Cipher before it is transferred to the Datto RMM Database.
- Data is never stored outside of the platform region that users select when signing up for the service. For customers on the Datto RMM EU (European Union) platforms, this means all data is stored in Ireland, for customers on US Platforms this currently means all data is stored in Virginia or Oregon, and for customers in APAC this means all data is stored in Sydney.

Datto Networking Data

Datto stores several types of customer and company data in the Datto Networking platform. Sensitive data is protected through secure encryption methodologies during transit and is stored securely in a VPC that is not exposed to the Internet. Datto retains confidential information to meet legal and regulatory requirements and confidentiality commitments. Requirements for data retention are specified contractually via the customer-specific Datto Terms and Privacy and policy.

Sensitive data is secured any time it must be transmitted or received via open, public networks. Encryption practices protect information involved in the Datto Networking solution from incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication, and replay.

Disclosures

Informed by Management there were no material incidents impacting the entity's service commitments reported and no material changes committed during the period under review.