datto
A Kaseya COMPANY

Datto, Inc.

RMM

SOC 3

Independent Service Auditor's Report on Management's Description of a Service Organization's System Relevant to Security and Availability

November 1, 2021 to October 31, 2022

ASCEND
AUDIT & ADVISORY

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") accompanying assertion titled "Assertion of Datto, Inc. Service Organization Management" (assertion) that the controls within Datto's RMM system (system) were effective throughout the period November 1, 2021 through October 31, 2022, to provide reasonable assurance that Datto's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability 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*.

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. Datto has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Datto is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Ascend Audit & Advisory's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. 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 management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Datto's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Datto's service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

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 were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the 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 the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Datto's RMM system were effective throughout the period November 1, 2021, to October 31, 2022, to provide reasonable assurance that Datto's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Ascend Audit & Advisory

ASCEND
AUDIT & ADVISORY

St. Petersburg, FL

January 1, 2023

ASSERTION OF DATTO, INC. SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Datto Service Organization's (Datto's) RMM system (system) throughout the period November 1, 2021, to October 31, 2022, to provide reasonable assurance that Datto's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) 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*. Our description of the boundaries of the system is presented in the 'Description of Datto, Inc.'s RMM System' and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period November 1, 2021, to October 31, 2022, to provide reasonable assurance that Datto's service commitments and system requirements were achieved based on the applicable trust services criteria. Datto's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in 'Principal Service Commitments and System Requirements'.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period November 1, 2021, to October 31, 2022, to provide reasonable assurance that Datto's service commitments and system requirements were achieved based on the applicable trust services criteria.

By: /S/ Jason Manar

Jason Manar
Chief Information Security Officer

January 1, 2023

DESCRIPTION OF DATTO, INC.'S RMM SYSTEM

Company Overview

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 US 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.

On June 23, 2022, Kaseya, LLC purchased Datto becoming the parent company of Datto under the name Kaseya, Inc. This combination of companies brought the best of both enterprises under one umbrella with the creation of IT Complete by providing better opportunities and an industry leading set of solutions to customers.

Services Overview

Datto's RMM solution include the following:

- Flexible, Automated Patch Management – Efficient and effective policy-based patch management for Microsoft and third-party software to maximize security and minimize downtime.
- Automation and Scripting – 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 helps streamline service delivery with scalable automation.
- Real-Time Monitoring – Datto RMM monitors all of the users' devices in real time including servers, VMs, ESXi, PCs, Laptops, and network devices.
- Network Topology Mapping – 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.
- 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 while Datto RMM isolates the device automatically to prevent the spread of ransomware while still maintaining contact with RMM.

System Description

Principal Service Commitments and System Requirements

Datto's Security and Availability commitments to customers are documented and communicated to customers in the Master Services Agreement and the description of service documents published on the customer-facing website. The principal Security and Availability commitments include, but are not limited to:

- Maintain appropriate administrative, physical, and technical safeguards to protect the security and availability of the Datto RMM 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 Controls at a Service Organization Relevant to Security and Availability.
  - International Organization for Standardization (ISO) 27001:2013 certification reviews.
- Use formal HR processes, including background checks, code of conduct and company policy acknowledgements, security awareness training, disciplinary processes, and annual performance reviews.
- Follow formal 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.
- Continuously 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 the retention period is reached and/or upon notification of customer account cancellation.

Datto establishes system and operational requirements that support the achievement of the principal service commitments, applicable laws and regulations, and other system requirements. These requirements are communicated in Datto's policies and procedures, system design documentation, and/or in customer contracts. Information Security policies define how systems and data are protected. These policies are updated as appropriate based on evolving technologies, changes to the security threat landscape, and changes to industry standards, provided any updates do not materially reduce the service commitments or overall service provided to customers as described in the customer contracts.

Datto regularly reviews the security, availability, and performance metrics to ensure these commitments are met. If material changes occur that reduce the level of security and availability commitments within the agreement, Datto will notify the customer via the Datto website or directly via email.

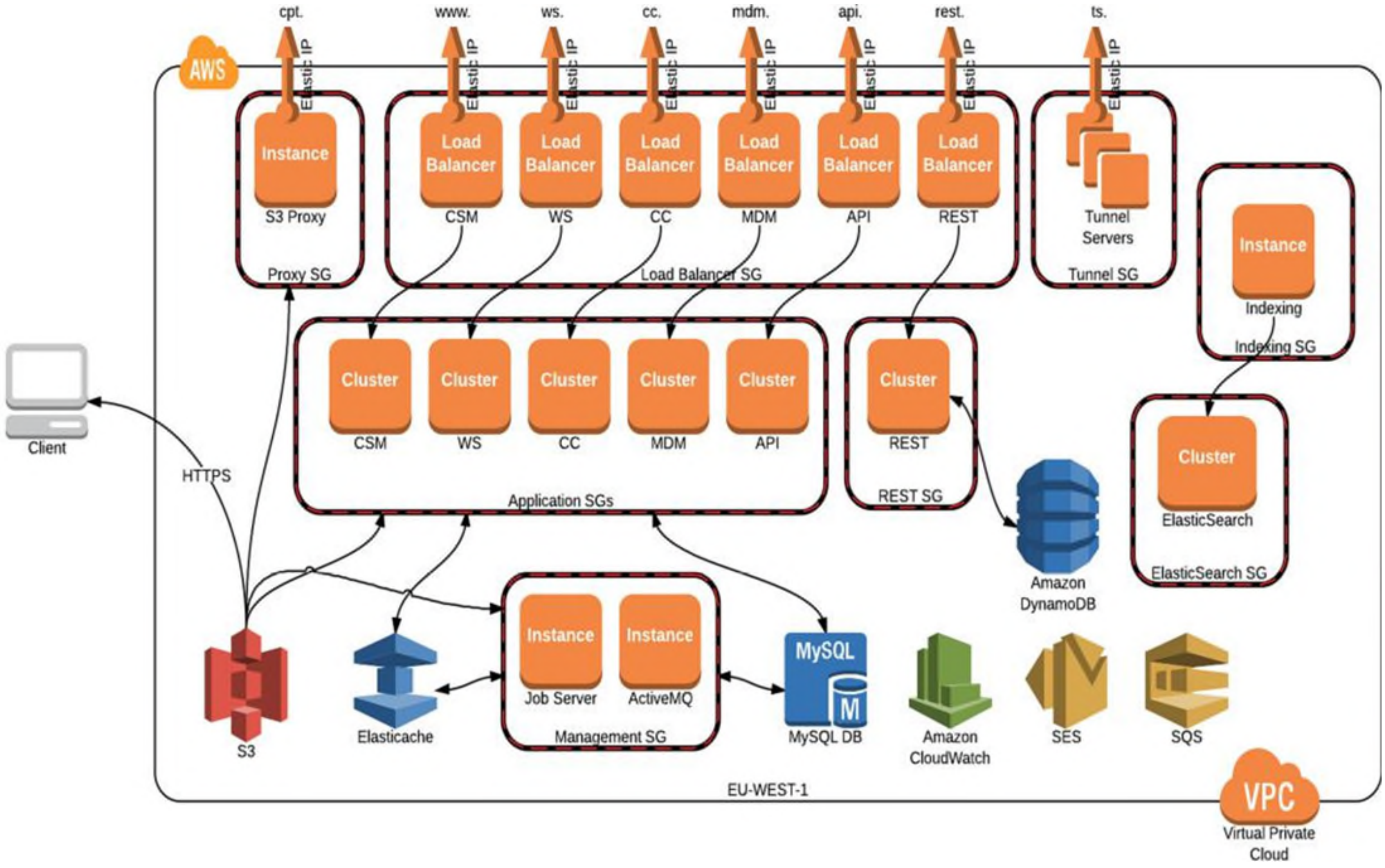
Components of the System

The System is comprised of the following components:

- Infrastructure (facilities, equipment, and networks)
- Software (systems, applications, and utilities)
- Data (transaction streams, files, databases, and tables)
- People (developers, operators, users, and managers)
- Procedures (automated and manual)

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 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.



Datto 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. 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 22 through a dedicated SSH Instance. Any servers which do not require external connections are therefore locked down and accessible only on port 22 via first connecting to a limited access VPN. 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 and Availability 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 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. AES 256-bit SSL 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.

Software

Datto has formalized policies and procedures that define requirements for managing application changes. This includes new development, change or amended application code management, and deployment to the production environment. Datto's Change Management is based on agile methodologies, with sprints working through a delivery pipeline. Approvals are obtained from at least two senior engineers who have not submitted the code being deployed.

Datto has formalized policies and procedures that define requirements for restricting access to the code repository. Datto's RMM source code is stored in a privately hosted Bitbucket repository. Access to Bitbucket is managed within AWS, requires private network access, and have Security Group ACLs applied to the infrastructure. Additionally, Bitbucket 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 analyzing and managing quality risk for the system.

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' private 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 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.

People

The organizational structure includes a separation of administrative, technology, finance, customer experience, general counsel, revenue, and marketing functions. The overall organization supports the framework for an effective control environment, and is comprised of the following functional areas:

Executive Management – provides strategic direction and leadership for Datto. Executive Management oversees and is ultimately responsible for all aspects of service delivery (including business development, marketing, and quality assurance), and all corporate services functions including but not limited to operations, finance, engineering, internal IT support, human resources, legal, facilities, and customer success.

Human Resources – is responsible for managing all functions related to recruiting and hiring, benefits, employee relations, performance management, resource management, and career assistance. The Human Resources team partners proactively with Executive Management and business units to ensure that all initiatives are appropriately aligned with Datto's mission, vision, and values. Datto is committed to equal opportunity of employment and all employment decisions are based on merit, qualifications, and abilities. Employment-related decisions are not influenced or affected by an employee's race, color, nationality, religion, sex, marital status, family status, sexual orientation, disability, or age. Datto endorses a work environment free from discrimination, harassment, and sexual harassment.

Internal IT Support (ITS) – this team provides IT services to all internal employees to the Datto ecosystem. ITS has overall responsibility and accountability for the enterprise computing environment, including single sign on, corporate software, corporate applications, operating system issues, software license requests, and network connectivity. IT personnel work closely with the end users of other functional areas to develop and implement guidelines and procedures to ensure that the enterprise computing environment is functioning both efficiently and effectively with regard to the Company's business objectives and requirements.

Internal Operations – provides support to all internal employees at Datto regarding workforce solutions, office services, facilities, and productions. Internal Operations assists with conference room support, office supplies, physical network infrastructure, HVAC, building access, and internal video projects.

Quality Assurance – seeks better methods and processes to help ensure the delivery of quality products. The Quality Assurance team is responsible for ensuring that Datto's suite of core backup products function correctly and achieve their intended business goals, ensuring quality in Datto's internal and external websites, and test all projects that come out of the research and development team.

Information Security management – avoids losses in confidentiality, integrity, and availability of Datto end user data and critical services through governance activities and maturation in people, processes, and technology. The Information Security team is responsible for incident response, intrusion detection, security information dissemination, vulnerability reporting and testing, red team operations, user awareness training, as well as governance, risk, and compliance.

DevOps Engineering – strives to innovate, architect, and implement solutions for the most interesting problems in the MSP business space. Datto SE continues to break into new areas of technology and expertise in order to keep Datto in the frontlines of the MSP market, while also providing solutions to problems that no other company has ever solved.

Partner Success – is focused on Datto's customers' overall health, product adoption, and driving improvement to the customer experience. Partner Success works through two main channels: reactive and proactive engagement. The reactive side is related to escalations, billing issues, credit requests, dial downs, and cancellations. Proactive campaigns focus on product adoption, releases, and general product awareness leveraging health and adoption score models.

Marketing – is responsible for the strategic deployment of the Datto brand and for building awareness through multiple media channels including the Internet, public relations, advertising, industry associations, and direct mail.

Finance – is primarily responsible for the accuracy of financial reporting. Finance personnel are responsible for corporate treasury matters, client invoicing and payment applications, payroll, and procurement processing. Finance provides support and assistance as needed to client services.

Procedures

Datto has the following formalized policies and procedures:

- Anti-Corruption Policy
- Asset Management Policy
- Business Continuity and Disaster Recovery Plan
- Change Management Policy
- Code of Conduct
- Confidentiality Agreement
- Data Governance Policy
- Electronic Data Destruction Policy
- Employee Handbook
- Enterprise Encryption Policy
- Hiring and Termination Checklist
- Incident Response Plan
- Information Risk Management Policy
- Information Security Policy
- Offboarding Process
- Onboarding Process
- Patch Management Policy
- Vendor Risk Management Policy
- Vulnerability Assessment Policy

Disclosures

No security incidents were detected or reported during the audit period that would affect Datto’s service commitments or system requirements.