Datto, Inc.

BitDam

SOC 3

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

December 1, 2021 to November 30, 2022

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 BitDam system (system) were effective throughout the period December 1, 2021 to November 30, 2022, to provide reasonable assurance that Datto's 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)*, 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 BitDam platform system were effective throughout the period December 1, 2021 to November 30, 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

St. Petersburg, FL

January 16, 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) BitDam platform system (system) throughout the period December 1, 2021 to November 30, 2022, to provide reasonable assurance that Datto's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (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 BitDam SaaS Protection 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 December 1, 2021 to November 30, 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 December 1, 2021 to November 30, 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 16, 2023

DESCRIPTION OF DATTO, INC.'S BITDAM SAAS PROTECTION SYSTEM

Company Overview

Datto, Inc. (Datto), founded in 2007, is a leading provider of enterprise-level technology to small and medium sized businesses. Headquartered in Miami, Florida, Datto serves an extensive and diverse client base, and has long maintained a reputation for excellence in both technologies and services qualities.

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.

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

The BitDam cloud enabled security solution proactively stops exploits contained in any type of attachment or URL. BitDam ensures high attack detection rates and delivers fast protection for the full range of content-borne attacks, before they are delivered.

System Description

Principal Service Commitments and System Requirements

Datto's Security, Availability, and Confidentiality 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, availability, and confidentiality commitments include, but are not limited to:

- Maintain appropriate administrative, physical, and technical safeguards to protect the security, availability, and confidentiality of the Datto BitDam 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, Availability, and Confidentiality.
- 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 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, confidentiality, and performance metrics to ensure these commitments are met. If material changes occur that reduce the level of security, availability, and confidentiality 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)

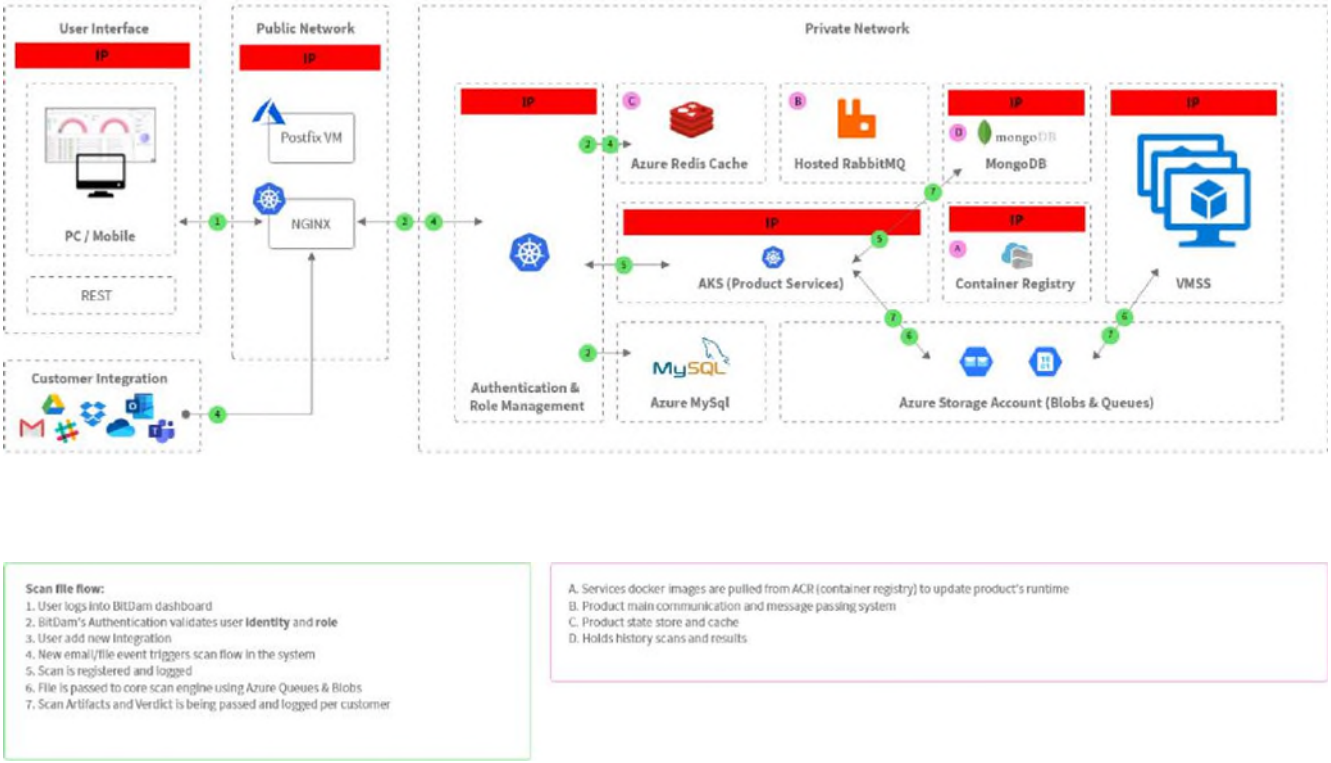
Infrastructure

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. Below appears the network architecture of the BitDam production environment.

BitDam'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.

Architecture Diagram for BitDam



Software

Datto has formalized policies and procedures that define requirements for managing application changes. This includes new development, changed or amended application code management, and deployment to production environment. Datto's Change Management is based on NIST SP 800-128: Guide for Security-focused Configuration Management of Information Systems. The process consists of request, planning, evaluation, documentation, notification, implementation, and resolution. Approvals are obtained by either product architect, departmental VP, VP of Engineering, CTO, or the CISO.

Datto has formalized policies and procedures that define requirements for secure application development. Datto continuously monitors for Systemic Security Issues (weak ciphers, insecure HTTP methods, cookies, session management, headers, etc.). Continuous checks for and repairs of these very common misconfigurations are conducted via vulnerability scanning processes. Datto's development process requires that source code to be peer reviewed before deployment to production.

Datto has formalized policies and procedures that define requirements for restricting access to the code repository. Datto's SaaS Protection source code is stored in a private Gitlab repository. Access to Gitlab is managed by Gitlab AD Groups.

All development occurs and is tested locally on the engineer's workstation. The local environment has been configured to mimic aspects of production. When necessary, additional staging and test systems are brought online in a completely 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. 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 analyzing and managing quality risk for the system.

Data

Datto stores various types of customer and company data in the cloud solution platform. Sensitive data is protected through secure encryption methodologies during transit and at rest. Unique encryption keys are utilized. 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.

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

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.

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 testing 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.

Software 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.

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.

Research and Development (R&D) **-** The R&D department is responsible for developing BitDam's products and the business services implemented within the production environment. This department includes five development teams as detailed below:

- UX: Responsible for the BitDam platform client-side components as well as all event tracking and analytics.
- Infrastructure & Tools: Responsible for developing specific tools and product frameworks for the R&D team to use.
- Backend: Responsible for developing BitDam cloud services that support product features.
- Core: Responsible for improving BitDam product detection capabilities and its effectiveness. Performs research and development of the BitDam core IP.
- DevOps: Responsible for providing BitDam with the required IT environments, production SaaS environments availability, security, and scalability. It operates the NOC that provides 24x7 control, monitoring, and resolution in case of failure. Works together with R&D during the go-to-live period to deploy the products according to the customer's needs and BitDam procedures.

Procedures

Datto has a Chief Information Security Officer (CISO) who is responsible for the design and oversight of security and privacy initiatives. The CISO reports directly to the CTO and indirectly to the Chief Executive Officer (CEO). The IT policy framework describes the procedures followed to ensure the performance of consistent processes over the security, availability, confidentiality, and operation of the BitDam Platform. All IT policies are reviewed on an annual basis, or more frequently as needed, by the CISO.

All employees are expected to adhere to Datto's IT policy framework as acknowledged during new hire onboarding and during annual security awareness training. The IT policy framework includes procedures that provide guidance on the consistent performance of controls and processes necessary to meet service commitments and system requirements.

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.