Datto, Inc.

AUTOTASK PSA

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

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 Autotask PSA 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 Autotask PSA 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

December 29, 2022

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) Autotask PSA 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 Autotask PSA 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

December 29, 2022

DESCRIPTION OF DATTO, INC.'S AUTOTASK PSA SYSTEM

Company Overview

Datto, Inc. (Datto), founded in 2007, is a leading provider of enterprise-level technology to small and medium sized businesses. Datto's cloud-based IT business management tool, Autotask PSA, is a complete 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.

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

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. Datto's Autotask PSA tool provides the following features:

CRM (Customer Relationship Management): Ability to track opportunities, manage contracts tickets, tasks, to-dos, and analyze sales performance in real-time. The ability to tap into service improvement, measurement, and client self-help tools allow customers to improve customer satisfaction.

Ticketing: Customers can track customer notes, contracts, incidents, and emails all in one place and manage an SLA (Service Level Agreement) timeline to uphold obligations to their customers. All these metrics are also tracked on customizable dashboards that keep users focused on mission-critical data.

Project Management: With automated project workflows, customers can consistently hit their targets with increased visibility around event tracking, integrated email, and project profitability assessment.

Invoicing: Key features include automatically applying time and expenses to any contract type, integrating timesheets with expenses with the preferred accounting system, and in-sourcing and outsourcing tickets from vendor partners to maximize resources. Billing disputes are minimal with the ability to include detail on an invoice that is customizable by the customer.

Reporting: Autotask PSA's reporting feature gives easy access to quickly see what is due with real-time updates and alerts to improve customer service. Customers can also set up internal best practices with automated workflows.

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 Autotask PSA 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 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:

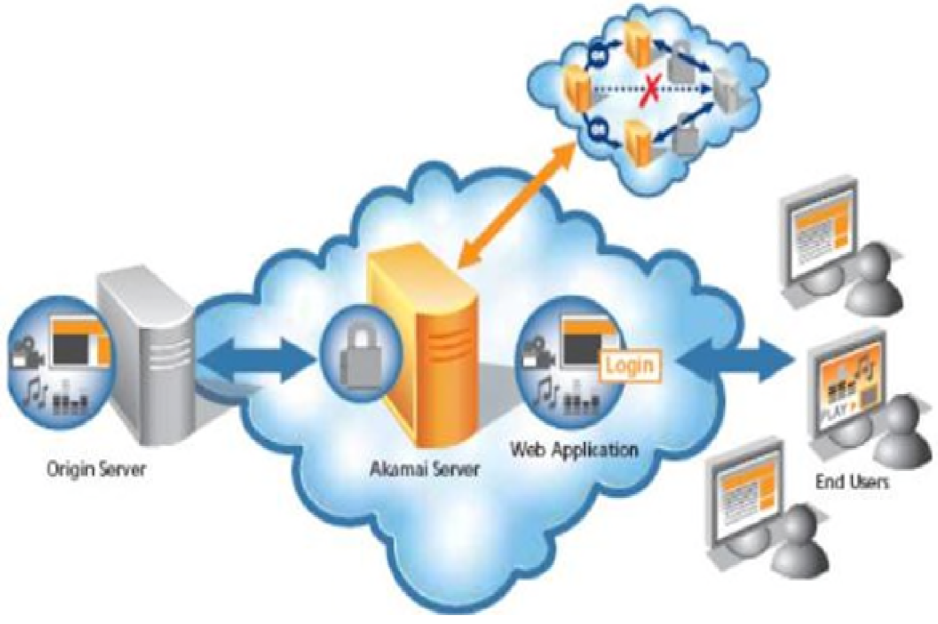
- Infrastructure (facilities, equipment, and networks)
- Software (systems, applications, and utilities)
- Data (transaction streams, files, databases, and tables)
- People (developers, operators, users, and managers)
- Procedures (automated and manual)

Infrastructure

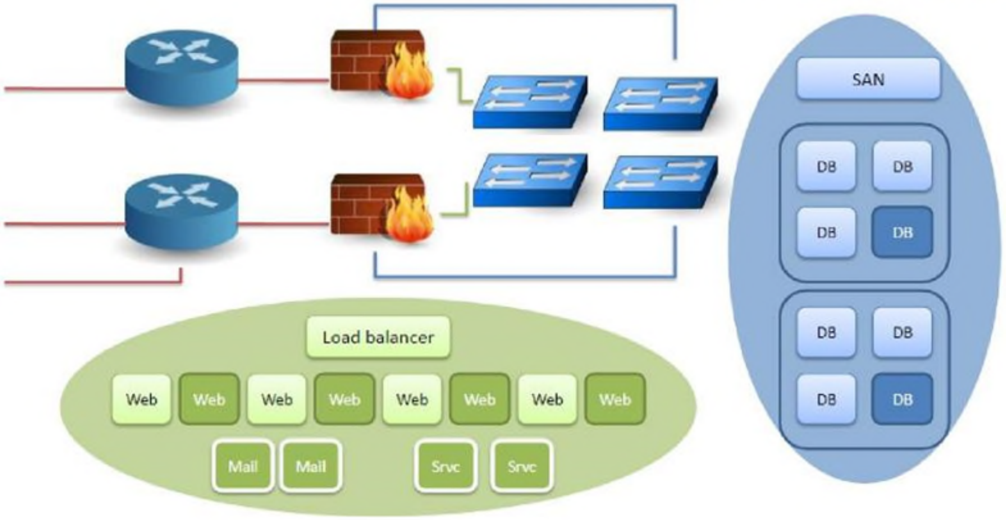
Autotask PSA operates on three resilient, high-availability data centers. These platforms exist in regions to provide increased performance for customers around the globe. At present the core platforms are hosted in the US, Germany, and the UK. All communication that needs to travel between regions is performed via secure SSH Tunnels or HTTPS connections. To help to achieve the required levels of resilience and scalability, Autotask PSA infrastructure is separated into multiple logical customer-facing zones. The services are separated into the following production zones: America West, America West 2, Australia, Limited Release, America East, America East 2, Spanish, Pre-release UK, Limited-release United Kingdom, United Kingdom, United Kingdom 2, Pre-release German, German, Pre-release European Union, and European Union.

The Autotask PSA service is additionally supported by a number of other infrastructures, service, and application components. The components of the Autotask PSA Cloud service are represented in the diagrams that follow.

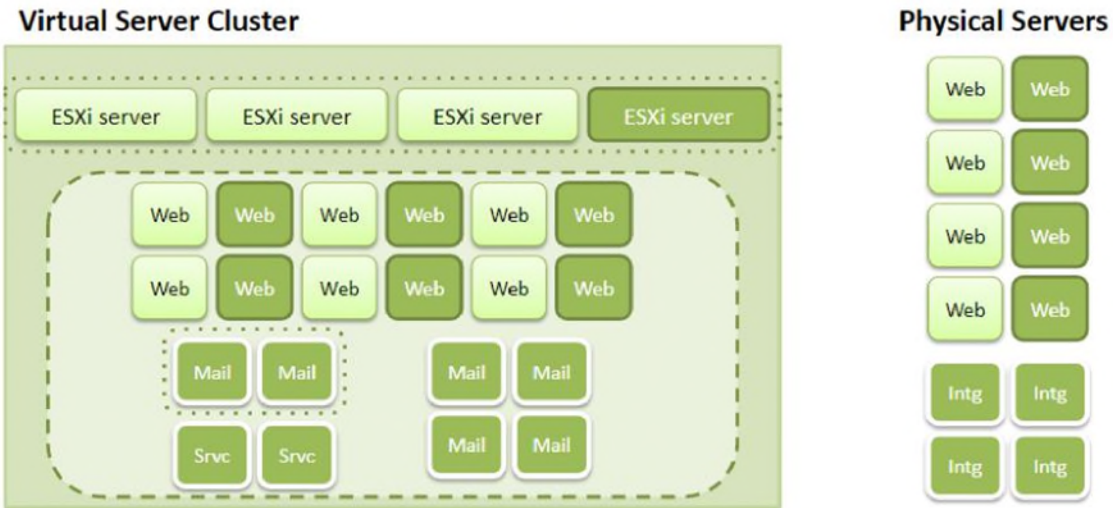
Data Center - Akamai



Data Center - Network



Data Center – DMZ



Datto’s System is a web-based information system. The Production Server side in the Company’s data center consists of:

Load Balancing – All of the core platform services (AT.net, Client portal, billing portal) exist as multiple servers within a virtual VMware environment and are themselves only accessible through dedicated Load Balancers. For the web-facing application, this load balancing is provided by redundant and available Netscaler appliances. Servers can be commissioned and decommissioned as required with no impact to the service itself.

Server instances – Autotask PSA uses Windows Server for the base operating system of the server instances. The version used has been specifically prepared, templated, and hardened 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.

File Storage – All attachments uploaded to the Autotask PSA platform are uploaded to separate storage tiers. This ensures durability of data, and also provides a highly available mechanism to securely serve these files back to end users.

Firewalls – Autotask PSA instances are, by default, closed for ingress via the use of strict firewall rules. By default, Autotask PSA publicly facing servers are only accessible via dedicated Load Balancers or SSH Tunnel instances. This means that access to these instances is only performed via port 443 for HTTPS secure web access. Any servers which do not require external connections are therefore locked down and not accessible externally.

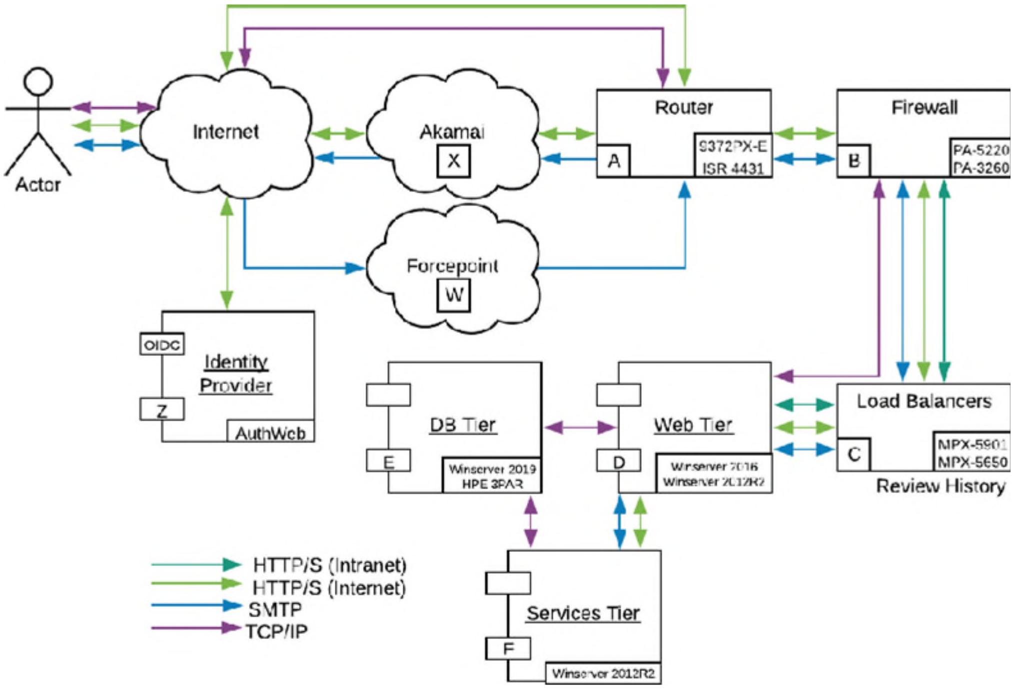
Software

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 benchmark standards to provide uniformity and consistency amongst the servers. Servers are layered and perform specific functions within the overall system, which includes web server, sessions state, and SQL server functional tiers.

- Windows Server 2012R2 - Application, web, and service servers
- SQL Server 2016 - Database storage for customer and data warehouse servers
- Azure DevOps Server (Team Foundation Server) - On premise code repository and version control

Data

- 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 different 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.



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.

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.

Technology – is responsible for the acquisition and maintenance of hardware, firmware, and backup systems that are responsible for the function of the Autotask PSA system. Technology provides on-call services that ensure that systems function within established guidelines and service level agreements that allow for a high level of uptime.

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 Autotask PSA 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.