Datto, Inc.

Backupify SaaS Protection

SOC 3

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

November 1, 2021 to October 31, 2022

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

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 Backupify SaaS Protection 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, 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 Backupify SaaS Protection 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) Backupify SaaS Protection 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, 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 Backupify 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 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 Backupify 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. Datto's Backupify SaaS Protection application, SaaS Protection, 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.

Backupify was acquired by Datto in 2014, effectively creating the first cloud-to-cloud total data protection platform. SaaS Protection is able to offer the most comprehensive options for backup, disaster recovery, and business continuity for companies of any size. Over 2.5 million business customers trust Datto-Backupify to protect billions of documents and email messages and over 98 petabytes of data.

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.

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 SaaS Protection solutions include the following:

- Automated Continuous Backup - Protect OneDrive, SharePoint, Teams, Gmail, Google Contacts and more with 3x daily, automated backups or perform additional backups as needed, at any time.
- Flexible Retention - SaaS Protection offers different data retention options to meet clients' individual needs.
- Admin Audit Log - Maintain a detailed record of all administrator and user actions from the admin dashboard.
- Ransomware Protection - Rollback data to a point in time before ransomware attacks.
- Recover Quickly – Flexible restore options allow users to recover lost data quickly while retaining file and folder structure in Microsoft 365 and Google Workspace (formerly G Suite).
- Easy Export - Export entire accounts or specific items in standard file formats.

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 Backupify SaaS Protection 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.
  - International Organization for Standardization (ISO) 27001:2013 certification reviews.
- Use formal HR processes, including background checks, code of conduct, 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

SaaS Protection 1.0 is written primarily in Ruby (Ruby on Rails web framework) and has infrastructure hosted partly in AWS and the Datto datacenter. 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 also backup current data at periodic intervals.

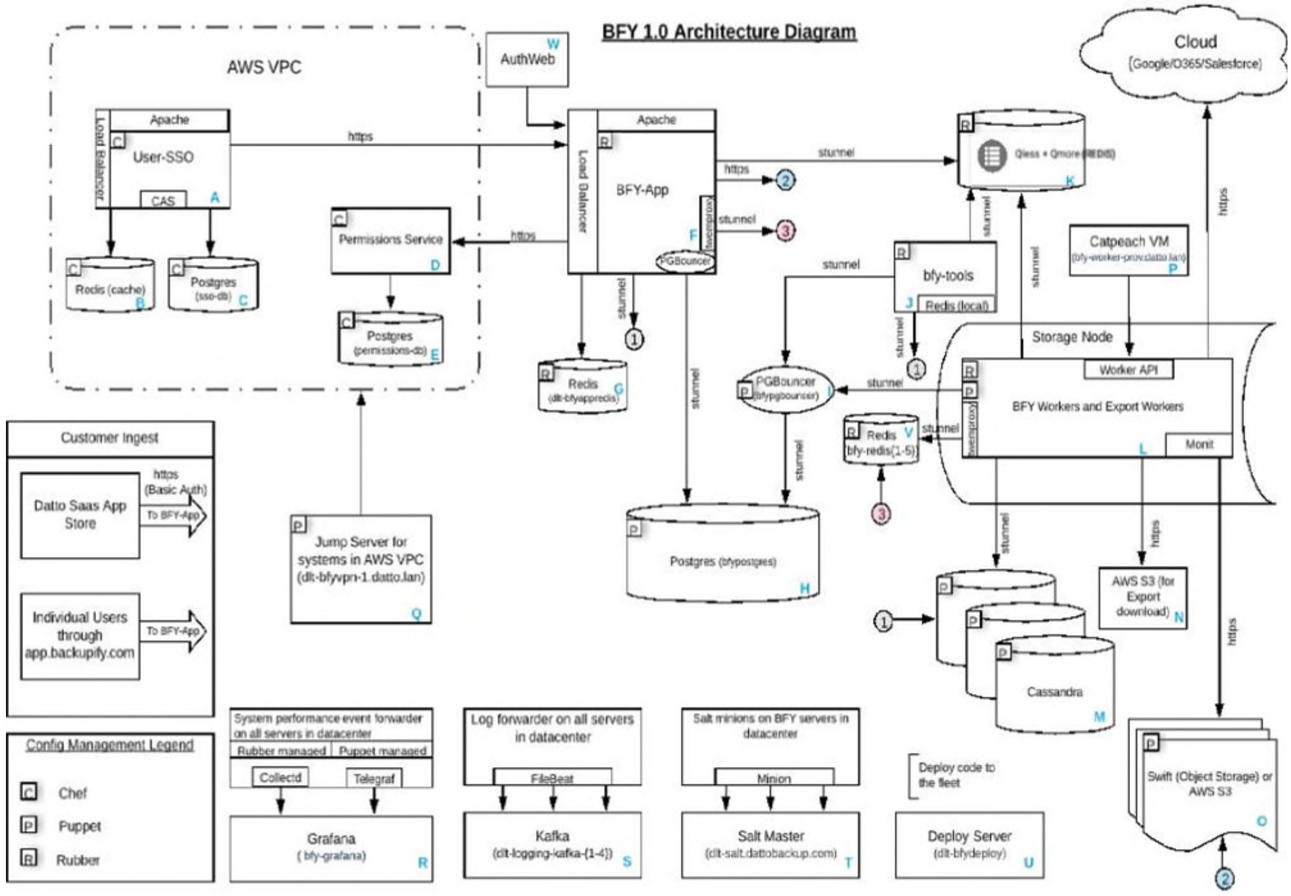
Depending on End User service levels and customer location, data might be backed up to object storage systems in the Datto datacenters or AWS (S3 service). The backed up data is also replicated within the Datto cloud for disaster recovery scenarios.

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 datacenter. 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 also 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.

Architecture Diagram for SaaS Protection 1.0



Letter	Name	Description
A	User-SSO application	User-SSO application is responsible for authenticating api users.
B	Redis Server	This database provides caching service for the user-sso web application.
C	Postgres (sso-db)	This is the database for the user-sso application that deals with user authentication/management.
D	Permissions svc	This is a service that is queried by the bfy-app application to determine user-roles.
E	Postgres (permissions-db)	This is the database for Permissions service that stores, among other things, user roles.
F	BFY-App	This is the application server that the user lands on after authentication. This application is responsible for generating user-views and also servicing user requests (from the browser). The BFY app servers are behind a HA proxy load balancer (dlt-bfyproxy).

(Continued)

Letter	Name	Description
G	Redis (dlt-bfyappredis)	This database provides caching for the bfy-app web application.
H	Postgres (bfypostgres)	This is the database for the bfy-app application that holds, among other information, user accounts, api-users, active services to be backed up, active exports, active restores, archived accounts, archived services, backup slots for various services, etc.
I	PGBouncer (bfypgbouncer)	PGBouncer acts as a connection pooler for the Postgres database that manages concurrent connections to the database.
J	bfy-tools	This server runs the Qless UI and is used for managing and monitoring jobs in Qless. The local redis instance on the server contains the no deploy list.
K	Qless + Qmore	SaaS Protection 1.0 works on a large queueing system (for job management) called qless. Qless stores its data in redis on VMs. Qmore is an extension of qless which hosts dynamic queues and queue priorities. Workers consistently reach out to Qmore to see if queue priorities have changed.
L	BFY Workers and Export Workers	BFY Workers (including Export workers) fetch the enqueued jobs from Qless and execute the job. Jobs could be backup, export, restore, etc. A scheduler called 'trident' (that runs on the workers) controls how many qless jobs run at a time.
M	Cassandra	The Cassandra database nodes/servers, among other things, stores some service data (e.g., email subject, body, etc.) and mappings of service data stored in Swift nodes or S3 buckets.
N	AWS S3	The worker stores backed up data for some customers (e.g., EMEA customers) in S3 buckets. Also, data from exports are stored in S3 buckets.
O	Object Storage data (Swift or AWS S3)	Swift nodes in the Datto datacenter store backed up service for most customers. Data for some customers is stored in AWS S3 buckets.
P	Catpeach VM	Catpeach application hosts api-endpoints that are used by Syseng to manage BFY workers.
Q	Jump Server (dlt-bfyvpn-1)	This is the jump server that gives SSH access to all the servers in the AWS VPC.
R	Grafana	Grafana is an analytics and monitoring platform for system performance logs from BFY infrastructure.
S	Kafka	Kafka is a stream-processing software platform for real-time feeds. This platform receives system logs from BFY.
T	Salt	Salt is a multi-tasking configuration management system for BFY infrastructure.

(Continued)

Letter	Name	Description
U	BFY Deploy (dlt-bfydeploy)	This box hosts scripts that are used to deploy new code to the fleet. The deploy scripts also reach out to bfy-tools to get a list of workers (from the no deploy database in the local redis instance in bfy-tools) that are unresponsive and must be exempted from deploy.
V	Redis (bfy-redis {1-5})	This server is the job caching server for the workers. The workers and the app servers use 'twemproxy' to proxy the connections to the redis servers.
W	Datto AuthWeb	Datto's single sign on solution enforces 2-factor authentication. User credentials are stored in AuthDB.

Supporting Infrastructure

Authentication Systems

- User-SSO
- AuthWeb and AuthDB (replacement for user-sso)
- LDAP (for terminal login to various servers)
- CentralBan
- stunnel (TLS mutual authentication)
- Database authentication on various databases (Postgres, Cassandra, Redis, etc.)

Infrastructure Administration

- Rubber
- Chef
- Salt
- Puppet
- Gitlab
- GitHub
- Netbox
- Ansible (for database servers)
- Vault (secrets management)
- AWX

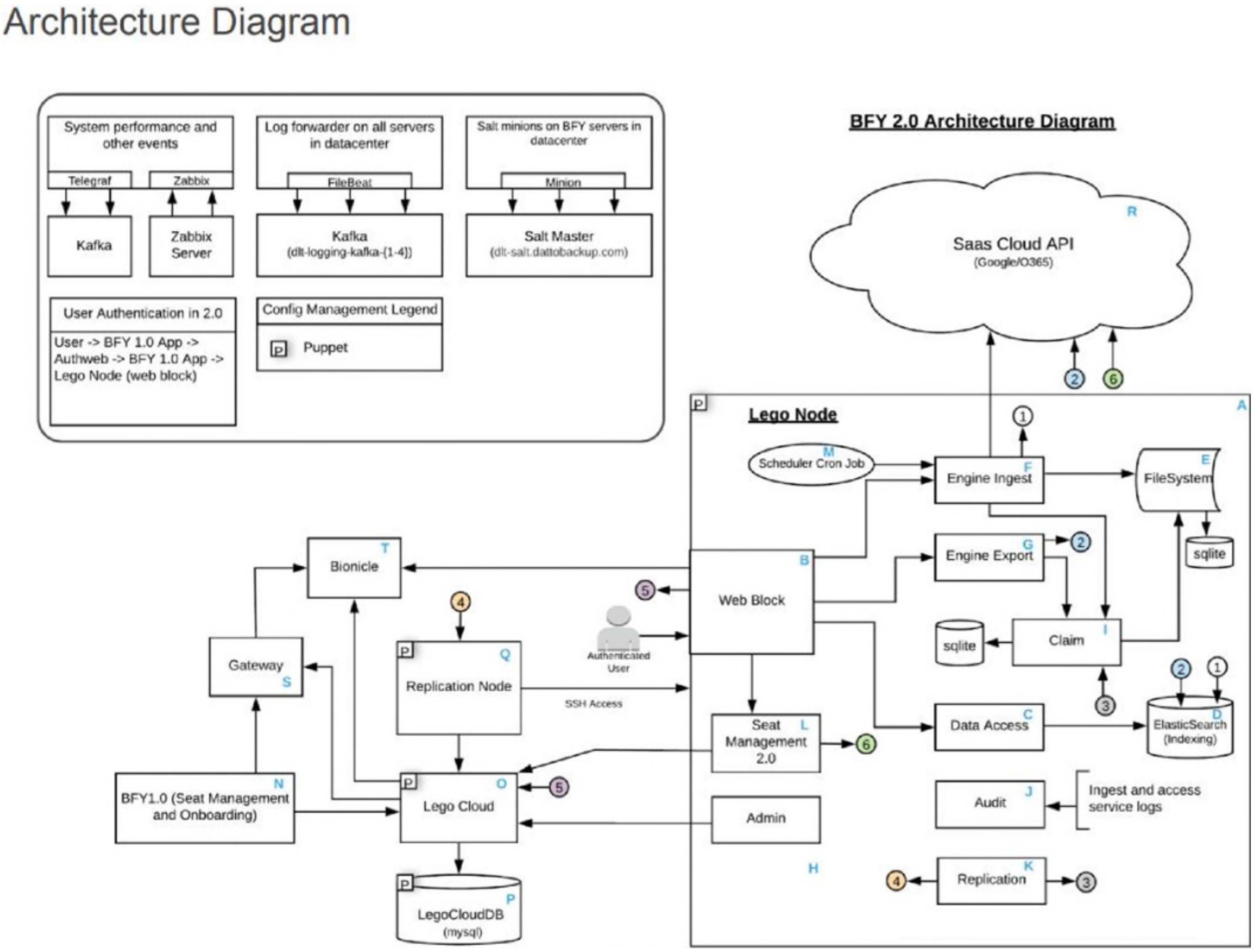
Monitoring

- Grafana
- Kafka
- ELK
- Foreman
- DCIM (for monitoring BFY workers in storage nodes).
- BFY-tools (for monitoring Qless jobs)
- Rapid 7

Security Scanners

- SBT dependency-check (for Scala dependency scanning)
- InsightVM (Vulnerability Scanner)
- Acunetix dynamic web application scanner
- Brakeman (for static scanning of code)
- bundler-audit (for ruby dependency scanning)

Architecture Diagram for SaaS Protection 2.0


Architecture Diagram
System performance and other events
Telegraf
Zabbix
Kafka
Zabbix Server
Log forwarder on all servers in datacenter
FileBeat
Kafka (dlt-logging-kafka-{1-4})
Salt minions on BFY servers in datacenter
Minion
Salt Master (dlt-salt.dattobackup.com)
User Authentication in 2.0
User -> BFY 1.0 App -> Authweb -> BFY 1.0 App -> Lego Node (web block)
Config Management Legend
P Puppet
BFY 2.0 Architecture Diagram
Saas Cloud API (Google/O365)
R
Lego Node
A
M Scheduler Cron Job
F Engine Ingest
E FileSystem
sqlite
G Engine Export
B Web Block
I Claim
sqlite
C Data Access
D ElasticSearch (Indexing)
L Seat Management 2.0
Admin
J Audit
Ingest and access service logs
H
K Replication
1
2
3
4
5
6
T Bionicle
Gateway S
Q Replication Node
Authenticated User
SSH Access
N BFY1.0 (Seat Management and Onboarding)
O Lego Cloud
P LegoCloudDB (mysql)

Letter	Name	Description
A	Lego App Node	The storage nodes host the Php-Symfony web application, scala services, and provides compute as well as storage resources for the users' data. In most cases around 100 customers are assigned to a storage node.
B	Web Block	Web Block is the web-frontend for BFY 2.0. It delegates tasks to various scala services running on the Lego node and displays the output to end users.

(Continued)

Letter	Name	Description
C	Data Access	Data Access service is the interface for querying items stored in Elasticsearch indexes.
D	Elasticsearch	Elasticsearch database stores indexed service data.
E	Filesystem	The filesystem contains a ZFS dataset (of each customer). The ZFS dataset is used for replication. The primary customer dataset includes directories corresponding to each service. Each service stores its data in its own directory. The metadata for the service is in a sqlite database that three (3) are present in each service directory.
F	Engine Ingest	Engine Ingest service is responsible for backups of service data.
G	Engine Export	Engine Export service is responsible for export and restore of service data. It connects to the SaaS Cloud API to restore the data back to the cloud (Google/O365). The exported data is written to the local filesystem where it is downloaded.
H	Admin	The Admin service manages check-ins with Lego Cloud and the tasks (e.g. provisioning new customers and services) that it gets from Lego Cloud, as well as facilitating processes such as customer pruning and customer migrations.
I	Claim	In the old design there were service level zfs datasets in addition to the customer level datasets. In this design, the Claim service was responsible for dynamically mounting and unmounting service level datasets for backup and exports. In the new design the service level datasets are replaced by individual directories that store each service's data. In this design, the claim service only maintains a cache of (customer level dataset) snapshots in memory. A common aspect in both designs is that the claim service maintains the state of unreplicated snapshots (in the sqlite database) and serves as a queueing mechanism for the replication service.
I	Claim	Note: New Lego nodes are configured as per the new design. Old Lego nodes still support the old design. The old nodes are being slowly migrated to support the new design.

(Continued)

Letter	Name	Description
J	Audit	The audit service stores event logs from the different services on the Lego node disk, e.g., backup, exports, restores, item success/counts, failure reason (stacktrace), etc.
K	Replication	The Replication service is responsible for replicating data from the primary Lego node to the replication node.
L	Seat Management 2.0	This service is the new version of Seat management in BFY2.0 and runs on the Lego node. Currently, it only supports seat management for M365.
M	Scheduler Cron Job	This cron job runs every five (5) minutes and backs up each service three (3) times a day, sending backup requests to the Engine Ingest service.
N	BFY 1.0 (Seat Management and Onboarding)	Seat Management is the final step in the customer on-boarding process (which also includes Service Side Scope Authorization). Seat Management dashboard in SaaS Protection 1.0 allows partners/customer admins to assign user licenses to domain users.
O	Lego Cloud	Lego Cloud service is used to delegate tasks (mostly Seat Management) to Lego nodes.
P	LegoCloudDB	Stores the (enqueued) tasks that must then be picked by Lego nodes. It also stores the current status of each Lego node. The Lego nodes share its status with the Lego Cloud via checkins.
Q	Replication Node	Stores the replicated data for a Lego node. Each primary node has a replication node that it then replicates the data.
R	SaaS Cloud API	This is the cloud-based API of the third-party SaaS services (e.g., Google and O365) that are backed up by Backupify.
S	Gateway	Gateway is responsible for providing aggregated information from 1.0 and 2.0 to portal (e.g., customers, users, and backup health) as well as [create and patch] customers and users to 1.0 and 2.0.
T	Bionicle	Bionicle is an admin support tool used to view data gathered from Lego cloud and gateway, as well as impersonate users in web-block.

Supporting Infrastructure

Authentication Systems

- AuthWeb and AuthDB (UserSSO for legacy API users)
- LDAP (for terminal login to various servers)
- CentralBan
- Database authentication on database (mysql)

Infrastructure Administration

- Salt
- Puppet
- Gitlab
- Netbox
- Ansible (CD solution for database servers)
- Vault (secret management)
- AWX

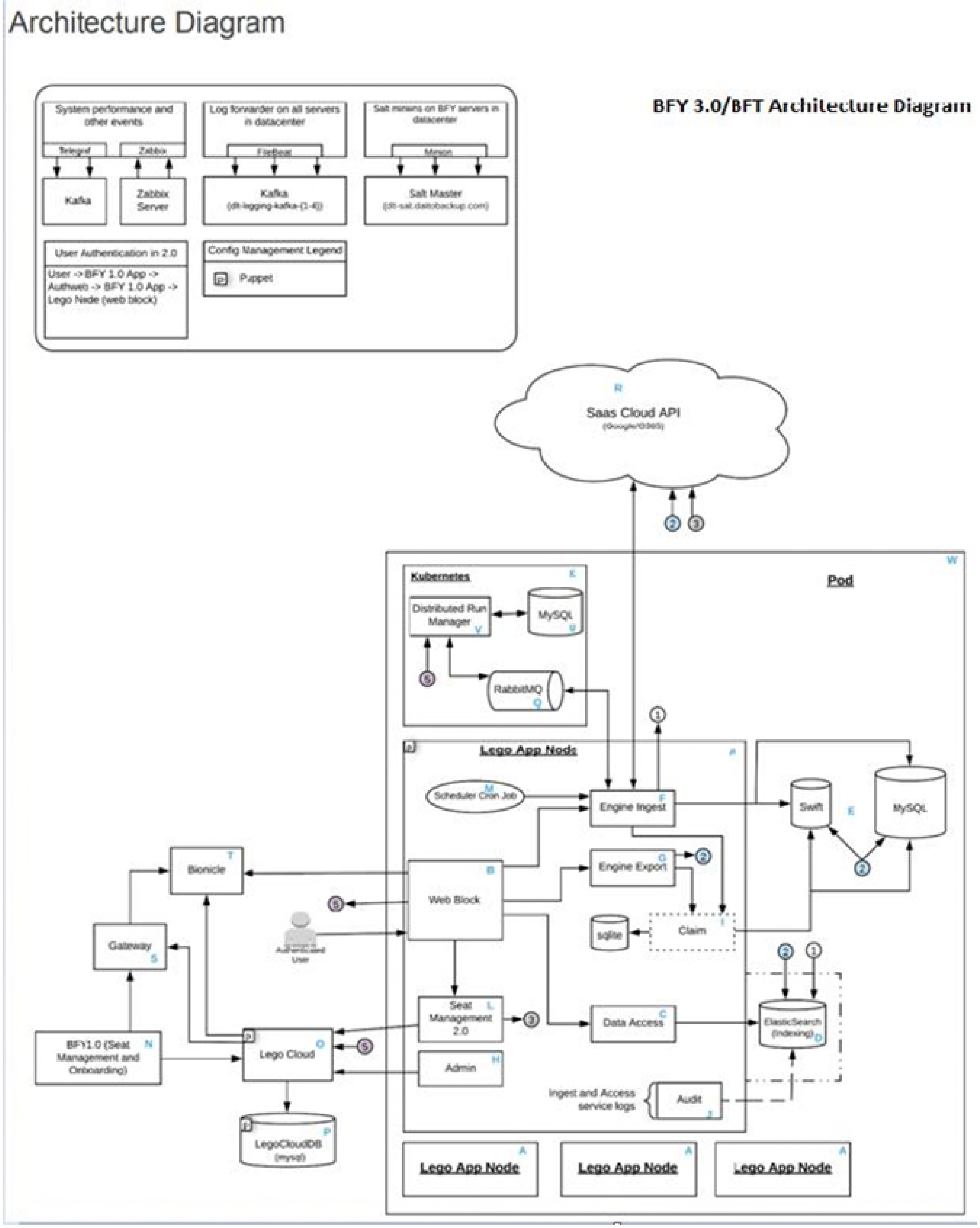
Monitoring

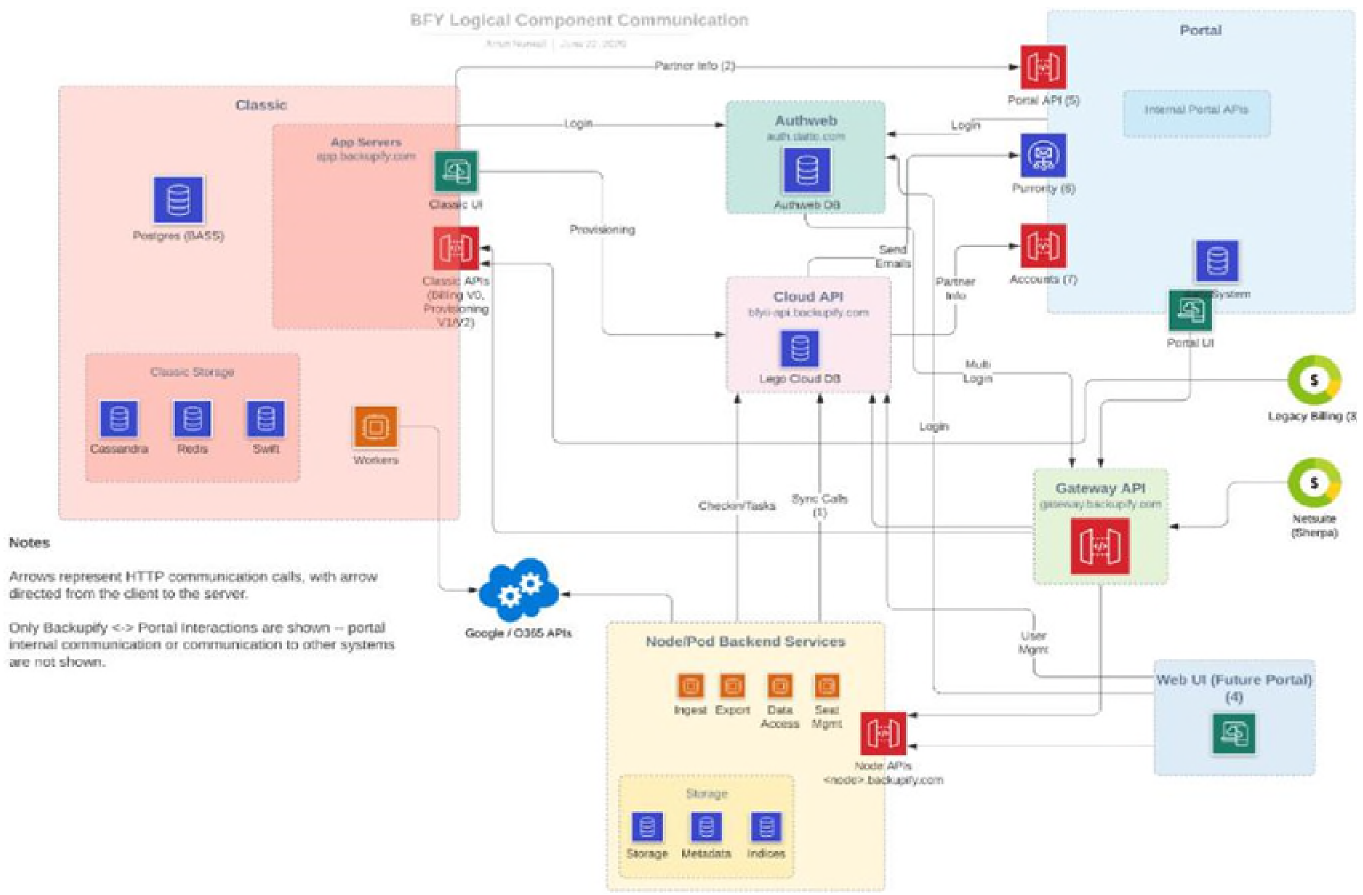
- Grafana (for data visualization)
- Kafka
- Zabbix
- ELK
- OpenTSDB
- Bosun

Security Scanners

- InsightVM (Vulnerability Scanner)
- InsightApsec dynamic web application scanner
- Snyk dependency scanning

Architecture Diagram for SaaS Protection 3.0/BFT





Notes

Arrows represent HTTP communication calls, with arrow directed from the client to the server.

Only Backupify <-> Portal interactions are shown -- portal internal communication or communication to other systems are not shown.

Letter	Name	Description
A	Lego App Node	The app nodes host the Php-Symfony web application, scala services, and provides compute resources for the users' data. A pod has many app nodes. Customers are currently assigned to specific nodes.
B	Web Block	Web Block is the web-frontend for SaaS Protection 2.0/BFT. It delegates tasks to various scala services running on the Lego node and displays the output to end users.
C	Data Access	Data Access service is the interface for querying items stored in Elasticsearch indexes.
D	Elasticsearch	Elasticsearch database stores indexed service data.
E	MySQL + Swift	MySQL and Swift are used together to store the customer backup data. Swift stores the encrypted data in packs while MySQL tracks where the individual files are. These MySQL and Swift clusters are unique per pod.
F	Engine Ingest	Engine Ingest service is responsible for backups of service data.

(Continued)

Letter	Name	Description
G	Engine Export	Engine Export service is responsible for export and restore of service data. It connects to the SaaS Cloud API to restore the data back to the cloud (Google/O365). The exported data is written to the local filesystem where it is downloaded.
H	Admin	The Admin service manages checkins with Lego Cloud and the tasks (e.g., provisioning new customers and services) that it gets from Lego Cloud, as well as facilitating processes such as customer pruning and customer migrations.
I	Claim	Manages snapshots of customer data. May be vestigial at this point, may be completely removed in the future.
J	Audit	The audit service stores event logs from the different services on the Lego node disk, e.g., backup, exports, restores, item success/ counts, failure reason (stacktrace), etc.
K	Kubernetes	Each pod has a Kubernetes server/cluster for hosting deployments of microservices to the pod.
L	Seat Management 2.0	This service is the new version of Seat management in BFY2.0 and runs off the Lego node. Currently, it only supports seat management for Microsoft Sharepoint and Teams by default.
M	Scheduler Cron Job	This cron job runs every five (5) minutes and backs up each service three (3) times a day, sending backup requests to the Engine Ingest service.
N	BFY 1.0 (Seat Management and Onboarding)	Seat Management is the final step in the customer on-boarding process (which also includes Service Side Scope Authorization). Seat Management dashboard in SaaS Protection 1.0 allows partners/customer admins to assign user licenses to domain users.
O	Lego Cloud	Lego Cloud service is used to delegate tasks (mostly Seat Management) to Lego nodes.
P	LegoCloudDB	Stores the (enqueued) tasks that must then be picked by Lego nodes. It also stores the current status of each Lego node. The Lego nodes share its status with the Lego Cloud via checkins.
Q	Rabbit MQ	Queueing service used for managing run queues operated by the Distributed Run Manager. (Future State)

(Continued)

Letter	Name	Description
R	SaaS Cloud API	This is the cloud-based API of the third-party SaaS services (e.g., Google and O365) that are backed up by Backupify.
S	Gateway	Gateway is responsible for providing aggregated information from 1.0 and 2.0 to portal (e.g. customers, users, and backup health) as well as [create and patch] customers and users to 1.0 and 2.0.
T	Bionicle	Bionicle is an admin support tool used to view data gathered from Lego cloud and gateway, as well as impersonate users in web-block.
U	MySQL (DRM)	MySQL for persistent storage of run information for the Distributed Run Manager (Future State).
V	Distributed Run Manager (DRM)	Microservice for managing all backup, export, and restore runs in a pod, allowing app nodes to pick up any job (Future State).
W	Pod	A collection of app nodes, data storage, Elastic Search cluster (Future State), and a Kubernetes cluster that work independently from other pods. Customers are assigned to a pod and pods can't read the data stored in other pods.

Supporting Infrastructure

Authentication Systems

- AuthWeb and AuthDB (UserSSO for legacy API users)
- LDAP (for terminal login to various servers)
- CentralBan
- Database authentication on database (mysql.)

Infrastructure Administration

- Salt
- Puppet
- Gitlab
- Netbox
- Ansible (CD solution for database servers)
- Vault (secret management)
- AWX

Monitoring

- Grafana (for data visualization)
- Kafka
- Zabbix
- ELK Foreman
- OpenTSDB
- Bosun

Security Scanners

- InsightVM (Vulnerability Scanner)
- InsightApsec dynamic web application scanner
- Snyk dependency scanning

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 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. 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 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.

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.

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 Backupify SaaS Protection 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.