Security Overview: Datto SaaS Protection

datto

Table of Contents

Overview

Datto, founded in 2007, is a leading provider of enterprise-level technology to small and medium sized businesses. Datto's SaaS Protection service is a cloud-based backup and recovery solution for application data including Google Apps, and M365. SaaS Protection is an easy-to-use solution that enables data backups from multiple SaaS platforms through a single user interface. Backup data is maintained in the Datto Cloud. Datto SaaS Protection provides:

- Protection from permanent cloud data loss due to insufficient native SaaS application recovery features.
- Protection from permanent data loss due to user error, malicious activity, or SaaS application outages.
- Ransomware recovery with the ability to restore user data to the moment before an attack occurred.
- Cross-user restore to retain former employees' data without continuing to pay for M365 or G Suite licenses.

Audit and Compliance

Objective:

To adhere to industry standard security, privacy, and confidentiality compliance frameworks.

Datto's Measures:

- The SaaS Protection product offering has been certified by independent auditors to meet SOC II Type II requirements with the Security, Confidentiality, and Availability Trust Services Criteria. Audit reports are updated on an annual basis.
- The SaaS Protection product has been verified by independent auditors to meet Google's OAuth API Security Assessment standards.
- Datto's GDPR posture can be found at https://www.datto.com/gdpr
  - For Partners storing data in the European Union,the SaaS Protection Terms of Use incorporates Datto's Data Processing Addendum (DPA). Partners may elect to store their backed up data in a European Union Datto Cloud datacenter. Please, see SaaS Terms for further information.
    1. Customers can select the location in which they would like to back up their data at the time of product setup.
    2. Customers can view the location in which their backed up data is stored in the product interface.
    3. Customers can select and manage retention configurations to manage their backed up data.

Organization of Information Security

Objective:

To foster a security-centric organization.

Datto's Measures:

- Datto employs a team of full-time, dedicated Information Security personnel that report to the Chief Information Security Officer.
- Members of Datto's Information Security team hold industry certifications including CISSP, CISM, OSCP, GREM, GCIA, GXPN, CISA, and GSNA.
- Datto has a comprehensive set of Information Security policies, that are reviewed and approved by senior management annually.
- All new hires are required to sign and acknowledge that they have received, read, understand, and will follow the Information Security Policy, Employee Handbook, and Confidentiality Agreement.
- All Datto personnel attend annual, formalized Information Security awareness training.
- ADatto provides annual first responder training which articulates best practices, what workflows to engage when evaluating an event that could become an incident, and when to engage them.
- Datto conducts criminal background checks on all U.S. employees, as well as select international employees, local jurisdiction permitting.

Physical Access

Objective:

To protect the physical assets that contain customer backup data.

Datto's Measures:

- Datto utilizes third-party data centers to house its production systems. Data resides within Datto owned and operated infrastructure or within AWS.
- Datto receives and reviews the SOC or ISO report of the third-party data centers on an annual basis, including the complementary subservice organization controls included within the report.
- Through its daily operational activities, Datto monitors the services performed by the third-party data centers to ensure that operations and controls expected to be implemented are functioning effectively.
- Facilities personnel are required to review the list of names and roles of those granted physical access to sensitive areas on a semi-annual basis to check for continued business need.
- Employees and contractors' access to facilities is removed upon termination.
- Physical access to facilities is controlled with electronic locks using access cards or pins.
- Physical access to sensitive areas is restricted to authorized personnel.
- Datto encrypts client backup data at-rest to protect customer information in the event of loss or theft.

Logical Access

Objective:

To ensure systems containing customer backup data are used only by approved, authenticated users.

Datto's Measures:

- Datto has formally documented policies and procedures defining requirements for granting, provisioning, and revoking access to data and systems.
- Unique user IDs are required for employee administrative access.
- Administrator access is limited to only authorized personnel.
- Quarterly reviews are performed to evaluate personnel access requirements.
- Datto utilizes an open-source password validation library to assess the quality of passwords.
- The web application automatically logs users out after a defined period of inactivity.
- Multi-factor authentication is required for remote access to Datto systems.

Data Transmission, Storage, and Destruction

Objective:

To ensure customer data is not read, copied, altered, or deleted by unauthorized parties during transfer/storage.

Datto's Measures:

- Datto encrypts client backup data at-rest using AES 256.
- Datto utilizes Transport Layer Security (TLS 1.2 or higher) for transmitting sensitive data over public networks.
- Prior to disposal, electronic media is securely wiped and sanitized to remove all data and software.
- The ability to perform customer backup data deletions is limited to authorized personnel.
- Data deletions are delayed from the initial request from the customer per the Terms of Use in an effort to protect confidential information from erroneous or malicious deletion requests.

Application and Development Security

Objective:

To ensure customer backup data remains confidential throughout processing and remains intact, complete, and current during processing activities.

Datto's Measures:

- Datto has a formal Software Development Life Cycle (SDLC) methodology that governs the development, acquisition, implementation, and maintenance of information systems and related technology.
- Software changes are documented, tested, and approved prior to migrating the change to production as part of the SDLC methodology.

- Peer code review is required prior to migration to production.
- Penetration tests of in-scope systems are performed by an external third party vendor, and by our internal penetration testing team, at least annually.
- Vulnerability scans of the production environment are performed at least monthly.
- Datto utilizes static code analysis tools and dependency scanners in the CI pipeline.

Logging and Monitoring

Objective:

To gain better insight into system metrics, ensure availability, and detect security vulnerabilities.

Datto's Measures:

- Datto utilizes an endpoint security platform that combines prevention, detection, and response in a single centrally-managed sensor to prevent attacks and expel adversaries to stop damage and loss.
- Firewalls are implemented to protect external access points from malicious attempts and unauthorized access, and are monitored to detect such attempts.
- Vendor security patches are evaluated, and critical patches are applied to key systems and applications in a timely manner after release.
- Datto utilizes a configuration management tool for deploying, configuring, and managing servers.
- Anti-virus software is installed on Windows and Mac OS workstations. Updates and signatures are pushed as they become available.
- Datto utilizes a network monitoring tool to monitor the health of the network and sends an alert if metrics are below defined thresholds.
- System capacity is monitored in order to plan for future requirements. Datto has deployed load monitoring tools that reflect and assess capacity levels and load balance for storage node performance. This customer backup data is constantly monitored via a dashboard display.
- Employee access to the Datto Cloud is logged and stored in the centralized log management system for later review as necessary.

Data Classification and Segregation

Objective:

To ensure appropriate safeguards are implemented, and access to customer backup data is only by approved users.

Datto's Measures:

- Datto is not, in the ordinary course, aware of the contents of customer backup data. Datto treats all customer backup data in the same manner. Datto does not mix customer backup data with its own internal data used for the administration of its business.
- Datto separates customer backup data in the Datto Cloud in a logical manner.

Incident Management

Objective:

In the event of any security breach of customer backup data, the effect of the breach is minimized and the Customer is informed properly and without undue delay.

Datto's Measures:

- Datto's Incident Response Plan outlines roles and responsibilities, containment and eradication strategies, restoration of services, breach notification guidelines, and postmortem analysis. The plan is reviewed annually and communicated to appropriate staff.
- Security incidents are logged and tracked in an incident tracking system. Support personnel and engineers review the incidents and security incidents are escalated to the Information Security team.
- The Incident Response recovery procedures are tested on an annual basis to evaluate its effectiveness and make any improvements.
- In the event of a data breach of customer backup data, Datto would notify the Datto Partner associated with the data, as soon as reasonably practicable, who would, in turn, be responsible for notifying any affected content owners.

Business Continuity and Disaster Recovery

Objective:

In the event of a disaster, Datto will be able to provide timely access, restoration, or availability to customer backup data.

Datto's Measures:

- Datto has a formally documented Business Continuity and Disaster Recovery Plan that is reviewed and updated annually.
- Annual tabletop exercises are performed to evaluate the effectiveness of the Business Continuity and Disaster Recovery policies and procedures.
- Datto's corporate internal systems maintain recovery strategies, such as data replication, and high availability strategies for critical data systems to assure the restoration of service.
- Datto's corporate internal systems utilize an automated backup system that is configured to notify personnel of failed backup jobs to assure the restoration of service in the event of an outage.

Best Practices for Datto Appliances

Objective:

Provide Partners with a guide to securely use and administer SaaS Protection.

Datto's Measures:

Datto provides a Knowledge Base that contains a large number of best practices documents on SaaS Protection setup and management:

- Security FAQ
- How to Perform Microsoft 365 Backup Restores
- How OAuth Works with Microsoft 365 Authentication
- The APIs SaaS Protection Utilizes to Backup Microsoft 365 Data
- A List of Permissions Necessary to Install SaaS Protection for Microsoft 365
- How to Perform Google Workspace Backup Restores
- How to Manage Administrators for Google Workspace

datto

Corporate Headquarters
Datto, Inc.
101 Merritt 7
Norwalk, CT 06851
United States
partners@datto.com
www.datto.com
888.294.6312

Global Offices
USA: 888.294.6312
Canada: 877.811.0577
EMEA: +44 (0) 118 402 9606
Australia: +61 (02) 9696 8190
Singapore: +65-31586291

Effective January 2021