datto | UNIFIED CONTINUITY

The Datto Cloud - Specifications

The Purpose-Built Backup & Recovery Cloud

The Datto Cloud is purpose-built for backup and recovery no matter where you operate. The benefits of the Datto Cloud go beyond a predictable cost model and offer unmatched security, performance and availability.

How many data centers does Datto use for backup replication and cloud-based recovery

There are currently 9 data centers across 7 countries and 4 continents.

What certifications are in place for the Datto Cloud?

	ISO27001	SOC 1 Type II	SOC 2 Type II	SOC 2 Type I
United States		•	•	
Canada			•	•
Australia	•			
Singapore	•			
Germany	•			
U.K.	•		•	
Iceland	•			

Encryption

- SIRIS uses AES 256 encryption
- Data is encrypted during the entire synchronization, storage and replication process*
  * Requires agent level encryption to be enabled
- Data is encrypted at rest via hardware encryption in the Datto Cloud
- MSP managed private keys can be optionally created for local and/or cloud backups*
  * Requires agent level encryption to be enabled

Secure management

Datto's Cloud Engineering team proactively monitors and maintains the servers of the Datto Cloud. This includes ensuring the health and optimization of hardware, overseeing OS updates, and conducting reactionary fixes for any security exploits either published or discovered. The Datto Engineering team is on-call 24/7 for emergency support.

- **Data Access:** Datto Cloud Engineering's access to node servers is granted via RSA SSH keys and two-factor authentication. Access to customer data requires a valid business purpose and has an audit trail.
- **Physical Access:** Physical access is guarded 24/7 by data center security personnel. Dual biometric and RFID badge scans with activity logging are required to access Man Traps and then the data center floor. Any visitors must be pre-registered, signed in by the site security personnel and escorted.

Redundant Data Centers

- Datto's cloud is composed of many data centers located in different countries. All primary sites are capable of providing users remote access to protected files and systems in the case of a disaster.
- The following locations offer secondary replication for up to 90 days of data for Datto SIRIS.
    - All US client data is first synchronized to the primary facility in Pennsylvania and then replicated in Utah*.
      * For devices who's subscription plan offers secondary replication
    - All Canadian client data is first synchronized to the primary facility in Toronto and then replicated to Calgary.
    - All UK client data is first synchronized to the primary facility in the UK then optionally replicated to Iceland.

Reliable Infrastructure

The Datto Cloud colocation facilities provide for various safeguards focused on fault tolerance and security. Some of those safeguards include:

- **Power:** Utility feed, N+1 generators, and 8 dual-module UPS battery systems supply Datto's servers.
- **Networking:** Multiple physical entry points and load balancing across three Internet Service Providers (ISP).
- **Cooling:** N+1 redundancy on chillers and N+25% on CRAC units, Industry-grade passive and active HVAC systems regulate temperature and humidity
- **Fire Protection:** Waterless FM200 systems use vapor to extinguish fires in 10 seconds while neither conducting electricity nor causing harm to occupants.

Organization of Information Security

Datto's Measures

- Datto employs 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, 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 formalized Information Security awareness training annually.
- Datto provides first responder training annually 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

Datto's Measures

- Datto utilizes third-party data centers to house its production systems.
- 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.
- Owners of sensitive areas of the facilities review the list of names and roles of those granted physical access to their areas on a semi-annual basis to check for continued business need.
- Terminated employees' and contractors' access to Company facilities is removed upon termination.
- Physical access to facilities is controlled with the use of 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 data in the event of loss or theft (AES 256).

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