

datto

# The Datto Cloud

Uncompromising Security, Constant Availability



## Secure Controls

Datto's data centers are compliant with the Service Organization Control (SOC 1 / SSAE 16 and SOC 2) reporting standards. Renowned as the predominant credential for data centers, the criteria for SOC auditing are set forth by the American Institute of Certified Public Accountants. The operational controls and activities of Datto's facilities are audited annually to maintain compliance.

## 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.

- **Encryption:** Data in transit from local Datto devices to the Datto Cloud is encrypted using AES 256-bit encryption. Certain Datto products have an optional local encryption feature that enables customers to encrypt backed-up data on their local devices; this enables them to transmit encrypted data to the Datto Cloud, which is stored in the Datto Cloud in an encrypted manner.
- **Data Access:** Datto Cloud Engineering's access to node servers is granted via RSA SSH keys and two-factor authentication.
- **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.
- **Data Residency and Data Centers for Datto Unified Continuity:** Datto devices that are purchased from Datto resellers located in the United States are typically set to backup to colocation facilities located within the USA, and such data remains in the USA unless the customer later changes such setting. Datto customers also can manage the retention settings associated with backups stored both on the Datto devices and in the Datto Cloud, in conformance with the service level purchased by the customer.

## Redundant Data Centers

Datto's cloud is composed of many data centers located in different countries. All US customer data is first synchronized to the primary facility in Pennsylvania.

A secondary location in Utah serves as means of replication for up to 90 days of data for the primary data center for Datto Siris and full, not optional, replication for SaaS Protection 2.0 datasets.. All primary sites are capable of providing users remote access to protected files and systems in the case of a disaster.

## Reliable Infrastructure

The Datto Cloud colocation facility located in the USA provides 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:** 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.
- **Certifications:** One or more of SSAE16/ ISAE3402 SOC 1 Type II, SOC 2 Type II, ISO 27001

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

©2019 Datto, Inc. All rights reserved.

Updated March 2019

Valid in the United States only.