datto | FILE BACKUP & SYNC

Datto File Protection

Security Architecture Guide

MANAGE™
PROTECT

Table of Contents

Dedicated Geo-Redundant Data Center Infrastructure....................1

SSAE 16 / SAS 70 and SOC2 Audits..2

Logical Access Security..2

Comprehensive Monitoring...2

Testing, Risk Assessment and Compliance..3

Data Encryption and Authentication 3

Password and Two-Factor Authentication Policies..........................3

Content Policies 4

Reporting..4

Dedicated Geo-Redundant Data Center Infrastructure

As opposed to the common virtualized approach to cloud services, wherein cloud service providers lease processing and storage capacity from Internet infrastructure providers, **all Datto File Protection hardware and software in each data center is 100% owned, operated, and managed by Datto**. In typical virtualized cloud environments, service applications and customer data actually share processing and storage platforms in a virtual time-sliced manner, resulting in a minimum of separation between independent operating domains. With the dedicated data center approach that Datto has invested in, nothing operates on any Datto File Protection hardware or software processing or storage platform except Datto File Protection services.

True 100% isolation of the Datto File Protection service eliminates the possibility of experiencing any service interruption, performance degradation, or malware infection that might otherwise be caused by adjacent applications. Combined with multi-level regional and data center redundancy, the File Protection infrastructure represents one of the most secure, reliable, and available cloud service architectures available today.

Datto File Protection uses a co-location model for deployment of Datto owned and operated equipment and software, utilizing the rack space, power, cooling, and physical security of major world-class SSAE 16 audited data centers. These facilities are classified as Tier 3 or better with N+1 fault-tolerant systems guaranteeing 99.982% availability. The Datto File Protection network architecture deployed to these facilities includes multiple levels of redundant internet links, application servers, switches, networking spanning tree failover, and storage arrays, thus ensuring high availability, failover support, and load balancing.

Datto operates data centers in several different geographical regions, including the United States, Canada, European Union and Australia, and is planning further expansion into other regions. Within each region, two levels of redundancy are provided. First, within each data center, redundant servers and file storage ensure that data center level failures can be isolated and resolved quickly. Second, within each region, at least two independent data centers are physically distanced and isolated from each other, thus providing protection from higher level data center failures, regional disasters, or broader Internet-related failures. This dual-level geo-redundancy ensures the greatest possible availability and protection against data loss.

The physical presence of data centers in separate regions also means that data does not leave the region; it stays in the United States for U.S.-based customers, in the European Union for EU-based customers, in Australia for AU-based customers, and in Canada for Canadian customers (in compliance with PIPEDA and local regulations). A new European privacy law, the General Data Protection Regulation ("GDPR"), went into effect as of May 2018. The GDPR fundamentally changes European privacy law and requires all companies that handle "personal data" of individuals in the EU to adopt more stringent privacy and security practices. Datto has made a substantial investment of time and resources to ensure its products and services are GDPR compliant.

Summary

Co-location model with HW and SW 100% owned, operated and managed by Datto

Geo-redundant, Tier 3, SSAE16 Audited data centers (two per region)

Complete, redundant, regional data set in each data center

Complete regional server setups in each data center

Data center redundancy using RAID6 mirrored backup with replication

Modular clustered server farms for service load-balancing, scalability, and failover protection

SLAs for availability (99.982%), response time, service restoral

SSAE 16 / SAS 70 and SOC2 Audits

In the rapidly changing landscape of cloud services, companies that handle sensitive information, such as in the legal, finance, and medical sector, find that they are under increasing scrutiny over their information processing controls. **Datto File Protection data centers are audited against both AICPA SSAE 16 / SAS 70 and ISAE 3402 criteria for system availability and security,** thus providing assurances regarding adequate oversight over the controls utilized in the processing of information. Similarly, Datto's own internal security controls are audited against SSAE 16 / ISAE 3402 criteria for employee policies, physical and logical access controls, intrusion detection and testing, service reporting, security incident procedures, training, change control, and configuration management.

Datto File Protection's SOC2 Type 2 examination report is issued in accordance with both the SSAE 16 attestation standards established by the American Institute of Certified Public Accountants and also the attestation standards established by the International Standard on Assurance Engagements (ISAE) 3402, known as "Assurance Reports on Controls at a Service Organization." Accordingly, Datto File Protection services can serve as a foundation upon which customers can build their SSAE 16 / SAS 70 / ISAE 3402 compliant data processing and storage policies and practices.

Logical Access Security

All Datto File Protection application servers are protected with OS security modules that apply Discretionary Access Control and Mandatory Access Control policies to all server processes, thus ensuring that no software process can be gainfully subverted.

All connection pathways within the Datto File Protection infrastructure are highly regulated as to the kinds of traffic that are allowed between various internal server endpoints. Any network traffic that does not meet the expected data flow patterns, in terms of source, destination, and traffic type, is immediately interrupted and reported to monitoring personnel through alerts. All known attack vectors are specifically prohibited.

Comprehensive Monitoring

All of the Datto File Protection regional data centers are monitored 24 hours a day, 365 days a year, by equipment service and operations staff, who also have immediate access to Datto File Protection engineering personnel in the event that it becomes necessary. Co-location with major world-class data center industry partners ensures that physical and environmental security is unsurpassed.

Datto File Protection utilizes dedicated software monitoring components that are designed to track and evaluate the operation of servers, networking equipment, applications and services within the Datto File Protection service infrastructure. This also includes monitoring of resources such as processor load, memory usage and disk space usage.

Alerts regarding performance or potential security issues are automatically distributed to several on-call staff via SMS and email.

All connection pathways within the File Protection infrastructure are highly regulated as to the kinds of traffic that are allowed between various internal server endpoints.

Testing, Risk Assessment and Compliance

Datto File Protection makes use of independent 3rd-party testing, analysis, and assessment services. Datto File Protection's multi-faceted approach to testing and risk assessment incorporates the following elements; ongoing 3rd party penetration testing of Web, Agent, and APIs, Periodic SAS/SSAE audits, and Daily Hacker Safe updates.

The General Data Protection Regulation (GDPR) became enforceable on 25 May 2018. The GDPR replaces the Data Protection Directive 95/46/EC and will help to standardize data the law of data protection across the Member States of the European Union. Datto is aware of its obligations as a processor under the GDPR and remains committed to helping to support its MSP Partners' and their clients' GDPR compliance efforts.

Datto, Inc. has certified certain of our services, for which we act as a data processor, under the EU-U.S. Privacy Shield Framework. For more information on Privacy Shield, please visit the U.S. Department of Commerce's Privacy Shield website at: https://www.privacyshield.gov/welcome

Datto File Protection is 100% compliant with all Security Rules specified in the Technical Safeguards, Administrative Safeguards, and Physical Safeguards from the Health Insurance Portability and Accountability Act (HIPAA) of 1996. Datto File Protection's Privacy Policy provides specific details regarding the policies implemented throughout Datto File Protection in order to comply with HIPAA. Furthermore, Datto File Protection engages health care provider customers as a HIPAA Business Associate through BAA agreements. Datto File Protection is also compliant with PCI DSS requirements, and therefore can be used as the foundation of a compliant infrastructure that end-customers might certify and deploy.

File Protection data centers are audited against both AICPA SSAE 16 / SAS 70 and ISAE 3402 criteria for system availability and security

Data Encryption and Authentication

All files handled by the Datto File Protection service are secured, both in transit and in storage, using 256-bit AES-encryption. Furthermore, in order to maximize the separation between teams, users, and files, a different unique rotating encryption key is used for each individual file. None of the encryption keys are stored "in the clear" in any non-volatile storage, but rather are encrypted and stored under the protection of a master key. Authentication is ensured through the use of certificate-based server authentication, which ensures that the user's agent will neither connect, nor cooperate, with any server other than those that comprise the Datto File Protection service. Even in the unlikely event of a successful attack on Internet DNS or routing infrastructure, which is quite outside the control of Datto File Protection or any other SaaS provider, Datto File Protection's certificate-based authentication will ensure that no malicious agent could successfully connect to the Datto File Protection service.

Password and Two-Factor Authentication Policies

Datto File Protection administrators are authenticated into the service against databases in the Datto File Protection service. **Administrators can set global policies to specify the password strength requirements and to enforce two-factor authentication.**

Two-Factor Authentication, also known as 2FA, is an extra layer of security. 2FA requires not only a password and username, but also something that the user has with them. This can be a physical "hard" token or a piece of information only they know or have immediately at hand, which may have been obtained through a "soft" token. File Protection Administrators can set policies to require 2FA as part of the login flow for an additional layer of access control. Datto File Protection supports the delivery of 2FA tokens through either SMS or with the use of an RFC-6238 compliant mobile app, which utilizes Time-based One-time Password Algorithm (TOTP) tokens (such as Google Authenticator).

Datto File Protection's 2FA feature also supports a **2FA IP Address Whitelist**. The 2FA IP Address Whitelist allows Admins to specify one or more source IP addresses that can be exempted from 2FA authentication requirements. This feature is commonly used to "whitelist" corporate headquarters or other remote offices, where there is reasonably high confidence that login attempts are from valid users that are physically located on company property, and behind company firewalls.

Content Policies

As users edit and save subsequent versions of a file, **the file versioning feature automatically retains the older over-written versions of all files for up to 180 days.** At any point during that period, Users are able to access old versions through the web portal. This feature has been particularly useful in circumstances where customers have been affected by ransomware type viruses. Because previous file versions are retained in the team account, inaccessible to PC-based viruses, users have the ability to recover damaged content.

Reporting

Datto File Protection features a set of advanced reporting capabilities that are specifically designed to support auditing for compliance with company policies. These advanced reporting features enable Datto File Protection Administrators to generate and export custom reports to establish audit trails and analytics on the following types of events:

- **Team Events** - Account management events for all users
- **Device Events** - including reports on Restore and Download events
- **User Access Events** - Device connections and portal access, with IP address filtering

Reports can be customized to include or exclude a variety of events based upon various criteria, such as date range, user name, IP address, and more. These filtered reports can then be saved for quick access and scheduled for automated report delivery via email. Reports can also be exported to XLSX format. When reporting on user accesses, any user access event can be mapped to specific source IP addresses, and can be viewed on a geographical map.

MANAGE™
PROTECT

Email: sales@manageprotect.com | **Phone:** 1300 657 500 (AU) | 0800 141 481 (NZ)

SYDNEY
506/55 Holt Street
Surry Hills Sydney 2010
Australia

MELBOURNE
Level 17, 31 Queen Street
Melbourne VIC 3141
Australia

AUCKLAND
PO Box 26370, Epsom
Auckland 1344
New Zealand