

UNITRENDS CLOUD FAQs

SAFETY, SECURITY, AND COMPLIANCE

Let the Unitrends Cloud do the work of off-site backup, DR, and compliance for you.

- Simplify your DR and archiving strategy with Unitrends backup appliances that connect to the Unitrends Cloud for long-term retention and disaster recovery spin-up.
- Save time with deeply integrated backup combined with our white glove service and award winning Customer Support.
- Easily meet compliance requirements with built-in reporting and automatically testing that compares recovery testing actuals with your RPOs and RTOs.



Purpose-Built Cloud

The Unitrends Cloud is purpose-built by Unitrends for off-site backup, disaster recovery, and long-term retention.

Unitrends Cloud Certifications and Compliance

Your data is safe and secure in the Unitrends Cloud. All data is encrypted in transit and at rest. The Unitrends Cloud is also compliant with many industry regulations, such as SOC 1 and SOC 2, HIPAA, CJIS, and GDPR.

Regular audits ensure that the colocation facilities and associated systems meet industry standards for physical security, encryption levels, network security, configuration management, monitoring, and other control areas. The Unitrends Cloud colocation facilities and systems audit report includes:

- Description of Controls Provided by the Data Center
- Overview of Operations
- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring
- Overview of IT General Controls
- Physical Security
- Environmental Controls
- Logical / Network Security
- Problem & Incident Management
- Change & Configuration Management
- Customer Setup and Implementation Controls
- Control Objectives and Related Description of Controls
- Complimentary User Entity Controls
- Tests of Operating Effectiveness
- HIPAA Controls Crosswalk

FAQs About Compliance, Certifications, Security, and Legal Requirements

- 1. What is the complete list of certifications and compliance requirements met by the Unitrends Cloud?**
 - Health Insurance Portability and Accountability Act (HIPAA) with BAA available.
 - SOC 2, a certification from the American Institute of CPAs (AICPA) that includes reports on security, availability, processing integrity, confidentiality and privacy.
 - Criminal Justice Information Services (CJIS)
 - General Data Protection Regulation (GDPR)
- 2. Can Unitrends provide a Business Associate Agreement (BAA) to help my business maintain HIPAA compliance?**

Yes, Unitrends will sign a BAA upon request. Contact Unitrends Support for assistance.
- 3. Where are Unitrends Cloud data centers located?**

Unitrends Cloud data centers are located in the United States, Canada, Germany, the UK, and Australia.
- 4. How does Unitrends maintain data sovereignty and meet each country's privacy regulations? Will my data remain in my geographic region or be at risk of cross-replication outside of the country?**

Unitrends Cloud data centers are compliant with each respective country's privacy regulations and data housing policies. Data stored in the Unitrends Cloud will remain in the originating country and will not be replicated outside of the country.

- 5. What indemnification is in place for third parties?**

Unitrends has master services agreements in place with all Unitrends Cloud third parties that provide indemnification in the event of a data breach. Affected customers will be notified if a breach occurs. No third parties host or have access to data in the Unitrends Cloud.
- 6. My organization needs to regularly audit all data. How do I audit data in the Unitrends Cloud?**

Contact Unitrends Support to schedule.

FAQs About DR Readiness and Customer Access

- 7. Does the Unitrends Cloud have a documented DR plan? Are DR procedures tested?**

Yes, the Unitrends Cloud has a documented DR plan that is tested at regular intervals.

- 8. What if there is an outage at the Unitrends Cloud data center? What kind of redundancy is built in?**

The Unitrends Cloud automatically replicates data to provide redundancy and safeguards against an outage. Redundancy is maintained within the same country as the originating data center to ensure privacy regulations and other in-country data housing policies are met.

- 9. Is the customer expected to perform any maintenance on servers at the Unitrends Cloud data center?**

No, Unitrends takes care of all maintenance, patching and upgrades for servers in the Unitrends Cloud. In a recovery scenario, Unitrends spins up servers on-demand from the customer's most recent replicated backup.

- 10. What is the overall bandwidth of the data center? Is the bandwidth provisioned between users?**

There is sufficient bandwidth in the Unitrends Cloud provided by multiple, redundant, OC-192 connections. The overall bandwidth available at any given time ranges from 10 gigabytes to dark fiber. The bandwidth is not shared between clients, ensuring that all users have the direct access they need.

FAQs About the Cloud Data Center Characteristics and Protocols

11. Is the Unitrends Cloud in a secure building?

Yes. All Unitrends Cloud data centers utilize a multi-layered security architecture including key cards and biometrics to prevent unauthorized access to the building and the data center. Customer equipment is secured in locked cabinets, cages, or suites. Security monitoring is done via closed-circuit television (CCTV) and is recorded digitally with over 90 days of history. CCTV cameras are located throughout the facility as well as externally to capture movement.

12. Is the building owned or rented by Unitrends?

Unitrends leases space and equipment in secure colocation facilities.

13. Is there redundancy in power and Internet in the data center building?

Yes. The Unitrends Cloud data centers have redundancy for critical systems and Internet connectivity to diverse backbones. Multiple routers are configured for fault tolerant routing and the facilities have 24x7 security and monitoring.

14. What is the network security setup?

The Unitrends Cloud network architecture is designed to provide security over external points of access and provide security to the network routers and switches. The ability to configure and update routers and switches located in the network is restricted to a limited number of authorized personnel. Routers are restricted to configuration changes from designated IP addresses. Access Control Lists (ACLs) are used on each router to restrict data traffic on the network devices. Only known addresses are allowed to connect to the routers.

15. Is there a fire suppression system in the Unitrends Cloud data centers?

Yes. Fire protection is provided via early detection smoke warning systems with dual action dry pipe and multiple zones for optimal coverage of the data centers.

16. Is the Unitrends Cloud climate-controlled?

Yes. The Unitrends Cloud data centers are climate-controlled to maintain a temperature of approximately 72 °F / 22 °C.

Getting Started

17. How do I get started with Unitrends Cloud?

Contact your Unitrends partner, or contact Unitrends Sales at sales@unitrends.com or 1.866.359.5411.

GET A CLOUD QUOTE

Unitrends increases uptime, productivity, and confidence in a world in which IT professionals must do more with less. Unitrends leverages high-availability hardware and software engineering, cloud economics, enterprise power with consumer-grade design, and customer-obsessed support to natively provide all-in-one enterprise backup and continuity. The result is a single source of support across a set of offerings that enable customers to focus on their business rather than backup. Learn more by visiting unitrends.com or follow us on LinkedIn and Twitter @Unitrends