Consult·Customize·Create

onQloud: A Security-First Approach to Backup and IT Management

Datasheet

www.onQloud.com

onQloud: A Security-First Approach to Backup and IT Management

During the first two quarters of 2021, 1,767 data breaches were registered, with a total number of records exposed of almost 19 billion. These numbers are alarming, and at onQloud, we take stringent steps to avoid any security threats to your data. We especially care for the safety and security of our clients, as many of them are using public cloud storage providers, which means vital data is being transmitted on an hourly basis with the help of our products.

In this white paper, we cover how we keep your data safe – with all of our products. We also provide recommendations on how you can additionally protect your information when using onQloud solutions.

Managed Backup Security

All the connections that **onQloud Managed Backup** performs to get your backups and recoveries done are SSL-encrypted by default. We consider it a mandatory level of protection. You can also enhance your data security on your own, and we provide a wide range of options for accomplishing this:

Backup Immutability. Immutability offers complete immunity to any changes to your data, providing a significant leap forward in keeping your data safe. An immutable backup is a copy of your dataset that cannot be modified, deleted, or overwritten. The data saved in an immutable storage format remains fixed due to the WORM (write-once-read-many) mechanism. This mechanism ensures that a backup dataset is locked safely away from any type of alteration.

Different permission levels for your administrators. Initially, you have a single administrator with root-level rights. But it is considered insecure to share root credentials with other people, So you can create separate administrator with different permission levels. For instance, you can assign an administrator for each company you work with, or you can limit their capabilities to monitoring only

Two-factor authentication. With this feature, you can be sure that, unless an intruder has access to both your phone and console credentials, they will fail to access the console to steal your data, and you'; always be able to see if someone tries to access the platform with your password.

IP allowisting. This option is useful when you have several static IP addresses being used to enter the onQloud Managed Backup console. In this case, you can add them to the list, and connections from any other IP addresses will be restricted, even with the correct credentials.

Protection from endpoint users. In some cases, users might accidentally delete or change some options that are vital for successfully creating backups, and onQloud Managed Backup provides options to avoid these mishaps. You can lock editing of backup and restore plans, or even hide the Managed Backup agent from end users, so that they won't have access to its GUI. This can be configure d in settings/ Global Agent options. You can also protect that console and CLI with a master password, which can be done under Endpoint Options.

Custom Password to restrict access to the backed-up data. When creating a backup plan, you can set a password that will be a mandatory requirement to recover the backed-up data. Without this password, no one will be able to access the information, asit will be encrypted. This is set in the **Compression and Encryption Options** step during the creation of new backup plan.

Tracking of all major actions within the console. You can always check what is happening in your console. For instance, you can see the IP address your administrators use to log in and check what they were doing during the last session. This can be seen in the **Organization/Audit Log.**

Please note: we don't store any of your data in our systems. All of the data is transferred to or from the storage location with the help of our Managed Backup solution; **no data is saved on our servers.**