724-832-1900
info@relyence.com

Relyence Corporation
540 Pellis Road, Greensburg PA 15601

Relyence Cloud Solution FAQs

How does the Microsoft Cloud secure Relyence data?

Microsoft's role in securing Relyence data is to ensure that no other Microsoft Cloud customers have unauthorized access to Relyence data.

To implement this, Relyence data is secured in the Microsoft Cloud in our dedicated Microsoft Azure storage account. This account is managed by the Relyence Operations Team. Access to this storage account is controlled through a unique storage access key, which is a key that only our Relyence Operations Team has access to.

In Microsoft Azure, each storage account is logically isolated from all other storage accounts. This logical separation with access being granted through the storage access key ensures that no other Microsoft Cloud customers can access Relyence data.

How does the Microsoft Cloud secure Relyence data processing?

Microsoft's role in securing Relyence data processing is to ensure that no other applications in the Microsoft Cloud share the same virtual memory and compute power that Relyence uses.

This control is enforced through the Azure Hypervisor. This technology is a mediator between the physical hardware in Microsoft's data centers and the virtual hardware that each virtual machine in the Microsoft Cloud has access to. It manages both memory and compute power (CPUs) such that each virtual machine has a dedicated virtual memory and virtual CPU that is not shared with any other virtual machine.

By doing this, the Azure Hypervisor allows each virtual machine in the Microsoft Cloud to operate as a standalone computer, therefore securing Relyence data processing from all other applications in the Microsoft Cloud.

Does Relyence encrypt data in its databases?

Data in Relyence databases is encrypted with Microsoft's Transparent Data Encryption (TDE) technology. This encrypts your data while at rest in our databases so if any individual or group was to gain unauthorized access to our databases, your data would be unreadable.

This encryption occurs on every save into the Relyence databases and decryption occurs on every read from Relyence databases. This service is managed by the Microsoft Cloud and is transparent to the Relyence application.

This encryption uses an AES-256 symmetric key where this key is managed by Microsoft. This key is protected by a built-in server certificate that is unique to each SQL Database server in the Microsoft Cloud. Additionally, Microsoft automatically rotates these certificates at least every 90 days.

Does Relyence encrypt data that is being transmitted to and from you?

All data transmitted between you and Relyence is encrypted. While in transit over the Internet, your data is encrypted with an HTTPS connection utilizing our SSL certificate.

Using our SSL certificate, your browser can confirm that you are communicating directly with Relyence servers and that the data being transmitted is only readable by you and Relyence servers.

Once your browser trusts that it is communicating with Relyence servers by verifying our SSL certificate with a certificate authority, your browser generates a symmetric key that will be used for encrypting data between you and Relyence servers.

This symmetric key is encrypted using Relyence's public key, which is included in the SSL certificate. Then, your browser transmits this encrypted symmetric key to Relyence servers, where it is decrypted with Relyence's private key. Note that the encrypted symmetric key can only be decrypted with Relyence's private key, and Relyence is the only entity that has this private key.

© Copyright 2019 Relyence Corporation

At this point, your browser and Relyence servers have a shared symmetric key that is only known to these two entities. All data transfer between Relyence and you is now encrypted and decrypted with this symmetric key, which ensures that data being transmitted is only readable by you and Relyence.

How does Relyence ensure that other Relyence customers cannot access your data?

We ensure that no other Relyence customers can access your data through the enforcement of tenant identifiers. When you first sign up for Relyence, your company is given a tenant identifier which is unique and cannot be changed.

All of your data, including users and your analyses, are tied to this tenant identifier.

This tenant identifier is not managed by your browser and all requests from your browser to the servers do not include this identifier. This ensures that there is no way to obtain your tenant identifier, someone else to obtain your tenant identifier, or spoof a tenant identifier while using Relyence.

This tenant identifier requirement ensures that at no point is your data available to other Relyence customers.

Does Relyence backup my data?

Relyence automatically backs up your data for you. These backups are retained for 30 days.

If you require data to be retrieved from a backup, our technical support team is available for help.

Is my data encrypted in Relyence backups?

Yes, all of your data is encrypted utilizing Transparent Data Encryption (TDE) technology.

What happens to my data when my Relyence Cloud Solution subscription ends?

When your Relyence Cloud Solution subscription ends, we retain your data for 3 months to allow you time to reactivate your Relyence license.

Does Microsoft have access to my data?

No, Microsoft does not have access to your data.

Does Relyence have access to my data?

No, Relyence is bound by our legal terms and does not have authorization to access your data.

Is Relyence deployed on a single-tenant or multi-tenant architecture in the Microsoft Cloud?

Relyence is deployed on a multi-tenant architecture in the Microsoft Cloud.

Even though the Relyence application potentially shares the same physical hardware as other applications, all data, processing, and memory for Relyence is logically separated from all other applications in the Microsoft Cloud through the usage or dedicated storage accounts and the Azure Hypervisor.

If you require a single-tenant architecture, please contact our sales team for pricing.

How physically secure are Microsoft data centers?

Microsoft data centers are tightly secured facilities that include many security elements in a defense-in-depth strategy. These security elements vary depending on the security layer and can include perimeter fencing, video camera, security personnel, secure entrances, locked server racks, and real-time communication networks.

The exact security specifications of each data center are held confidentially by Microsoft.

Other questions?

Contact us! Give us a call at 724-832-1900 or email us at support@relyence.com.

© Copyright 2019 Relyence Corporation