rillion

White Paper

Data Security
in Rillion One

Introduction

Businesses all over the world use Rillion to streamline their financial operations.

As focus within IT shifts from producing services to delivering services, cloud-based systems are becoming increasingly popular as a preferred technology for all types of businesses.

This whitepaper describes the data security implemented for the cloud-based service Rillion One.

Considerations for the cloud

Encryption

Encryption ensures that data remains confidential and can be enforced either at the transport layer (In Transit) or when the data is stored (At Rest).

The following user scenarios are implemented for Rillion encryption:

1. In Transit Client to Web Application
3. In Transit Server to Backup Vault
4. At Rest Customer Data
5. At Rest Backup Data

In Transit Client to Web Application

Communication between the user browser and the Rillion One service is encrypted with the TLS protocol to achieve a secure and private connection.

In Transit Backup Data

All server systems in Rillion One are hosted on the Azure platform from Microsoft and utilize the Azure Backup Service. Data in transit during backup from the Rillion environment to the Azure Recovery Service Vault is encrypted with AES-256 encryption.

At Rest Customer Data

Rillion One server systems utilize the Azure Storage Service with encryption (SSE). This means that all storage, regardless of server type, is encrypted while at rest at the storage level in the virtual Azure infrastructure. All data written to the Azure Storage subsystem is encrypted with AES-256 encryption and keys are stored and managed by Microsoft internally.

All customer content in the Rillion One platform is stored using Azure Local Redundant Storage (LRS), containing multiple copies in the same data center environment to minimize risk of data loss or physical data corruption.
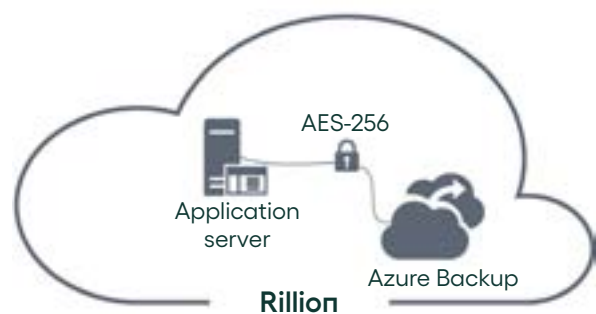
At Rest Backup data

All server systems in Rillion One are hosted on the Azure platform utilizing the Azure Backup Service protected with AES-256 encryption at rest.

The customer's data is stored in states once a day which can be recovered if needed. Recovery is available for 30 days. The customer must ensure that the original content from connecting systems/ERP:s or other Customer systems content is available outside Rillion One and possible to re-read into Rillion One for further handling.

All backup data is stored on Geo Redundant Storage (GRS) that is replicated across multiple geographically separated Azure regions and data centres.

All backup data stored in the Azure Recovery Service Vault is encrypted with AES-256 encryption.

AES-256

Application server

Azure Backup

Rillion

Connectivity

As a public cloud service Rillion One is available from anywhere on the Internet, but with all connections passing through our access security layer for security and confidentiality.

System components such as servers and related services performance are monitored in real time by Rillion One personnel during Business Hours on Business Days. Various system alarms will trigger on predefined levels supporting quick handling of critical system issues. The availability of Rillion One is monitored and measured every 5 minutes.

Data Capture connections
Rillion One utilizes third-party software for data capture - the process of extracting data from invoices. The connections to these services are either via the service API using a HTTPS connection or FTP (File Transfer Protocol) transfers.

User connections

User connect to Rillion One using a web browser over a TLS encrypted HTTPS connection.

Integration connections

Information exchange with external systems such as ERP or middleware is either file-based, with files transferred over FTP, or web-based utilizing Rillion One or a third-party Web Service over a TLS encrypted connection.

rillion

Authentication and Authorization

Rillion One uses authentication and authorization to positively identify users and give them access to resources. Authentication pertains to the process of validating a user's identity. Authorization pertains to the process

of granting a user permission to access specific resources when their identity is verified.

Rillion One applies Basic authentication which is an authentication scheme built into the HTTP protocol. .

Physical security

All data stored in Rillion is located in Microsoft Azure datacentres. Microsoft designs, builds, and operates data centres in a way that strictly controls physical access to the areas where the data is stored. A layered approach to physical security is used to reduce the risk of unauthorized users gaining physical access to data and the data center resources. Data centres managed by Microsoft have extensive layers of protection: access approval at the facility's perimeter, at the building's perimeter, inside the building, and on the data center floor.

Physical security reviews are conducted periodically of the facilities to ensure the data centres properly address Azure security requirements. Upon a system's end-of-life, Microsoft operational personnel follow rigorous data handling and hardware disposal procedures to assure that hardware containing data is not made available to untrusted parties. A secure erase approach is used for media that support it. For devices that can't be wiped, a destruction process is used that destroys the media and renders the recovery of information impossible.

The Azure infrastructure is designed to meet a broad set of international and industry-specific compliance standards.

Conclusion

Rillion enforces industry leading standards for data security and network protection. Moving to the cloud services with Rillion offers equal or greater data security compared to onsite installations. By integrating its cloud hosting on Microsoft Azure, Rillion can offer robust and reliable cloud services with the highest level of security for its customers.

As the creator and sole owner of the Rillion code base, Rillion technicians offer the best possibleservice and support for cloud services as well as delivering agile and responsive development for new releases.

Companies can focus less on infrastructure maintenance and spend more time to focus on core business processes while benefiting from the centralized services managed and provisioned by Rillion.

AP automation with Rillion saves time, lowers cost and improve efficiency gains for over 3 000 clients worldwide.

For more details on Rillion's solutions, and to get in touch with Rillion's experts to see how Rillion can help you redefine your AP process globally, visit: www.rillion.com