rillion

White Paper

Data Security in Rillion

Introduction

Businesses all over the world have discovered Rillion and use Rillion's purchase-to-pay (P2P) products to streamline their financial operations.

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

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

> ***The security in our cloud service is our top priority and is crucial for the safety of our customers***
>
> Per Nilsson
> Head of Online Operations

Our Cloud platform

To offer industry leading data security and protection, Rillion is delivered on the Microsoft Azure cloud platform.

For more information, see microsoft.com

Considerations for the cloud

Designing the cloud solution led Rillion to consider the following aspects of data security:

Encryption

To ensure that data remains confidential at all times, data encryption must be implemented in-transit and at-rest.

Connectivity

To use the services from any device with an Internet connection, cloud connectivity needs to be robust and secure.

Authentication and Authorization (AA)

To deliver flexible yet secure authentication methods while maintaining principle of least privilege.

Logging

Logging enables universal monitoring and audit trails for compliance.

Network protection

Network protection is a key component in delivering cloud-based services available over public networks.

Customer Isolation

Customers using a cloud service need to be clearly isolated from each other to prevent leakage of unauthorized data between customers.

Physical security

Physical security is crucial in protecting customer data from unauthorized access

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
2. In Transit Internal Server to Server
3. In Transit Server to Backup Vault
4. At Rest Customer Data
5. At Rest Backup Data

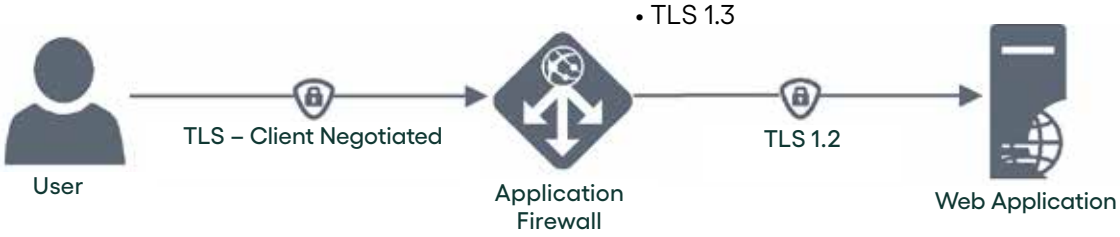
1. In Transit Client to Web Application

Communication between the user browser and the web application firewall layer (WAF) is negotiated to the highest mutual TLS configuration to achieve a secure connection.

The proxied connection from WAF to internal web application server is encrypted with: TLS 1.2 ECDHE_RSA_WITH_AES_128_GCM_SHA256.

Supported protocols and ciphers on client side are:

- TLS 1.2
- TLS 1.3



2. In Transit Internal Server to Server

Internal server-server communication can be either access to files saved in the cloud or to the cloud service database.

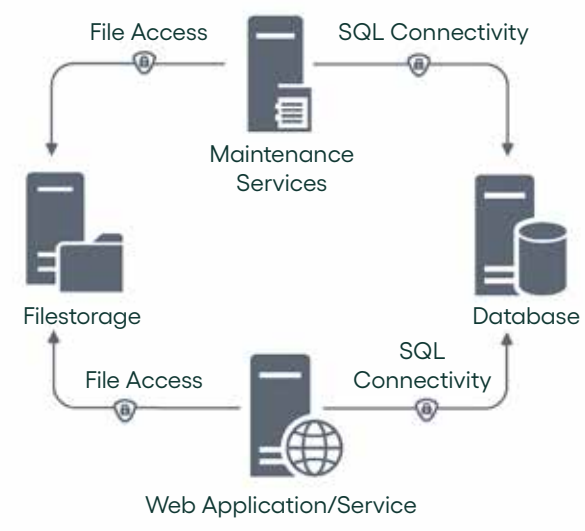
Access to cloud files

Customer file data is accessed by the web application/service and the maintenance service responsible for import/export of data. File access takes place over the SMB3 protocol using HMAC-SHA256/AES-128-GCM encryption.

Access to cloud database

Customer databases are accessed by the web application/service and the maintenance service responsible for import/export of data.

All SQL connections are encrypted using RSA-SHA256/AES-128-GCM.



3. In Transit Backup Data

All server systems in Rillion are hosted on the Azure platform from Microsoft and utilize the Azure Backup Service.

Data in transit during backup from the Rillion environment to Azure Recovery Service Vault is encrypted with AES-256 encryption.

4. At Rest Customer Data

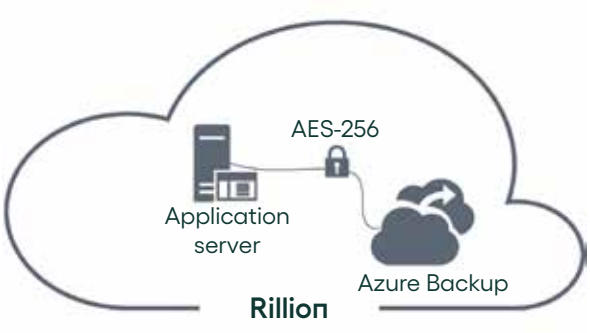
Server systems in Rillion are hosted on the Azure platform from Microsoft utilizing the Azure Storage Service with encryption (SSE). This means that all storage, regardless of server type, is encrypted while at rest at the storage level in the virtual Azure infrastructure.

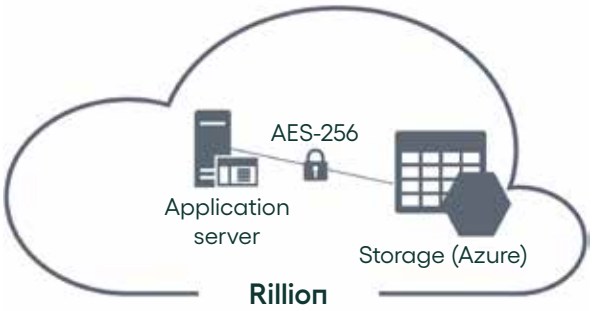
All data written to the Azure Storage subsystem is encrypted with AES-256 encryption and keys are stored and managed by Microsoft internally.

5. At Rest Backup data

All server systems in Rillion are hosted on the Azure platform from Microsoft utilizing the Azure Backup Service.

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





Connectivity

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

The following diagram shows the three main types of connections associated with a Rillion customer environment.

1. Data Capture connections
2. User connections
3. Integration connections

1. Data Capture connections

Data capture, such as import of invoice images, are normally accomplished with SFTP (SSH File Transfer Protocol) but may in some cases also use Rillion Web Service APIs.
In both cases the connection is encrypted.

2. User connections

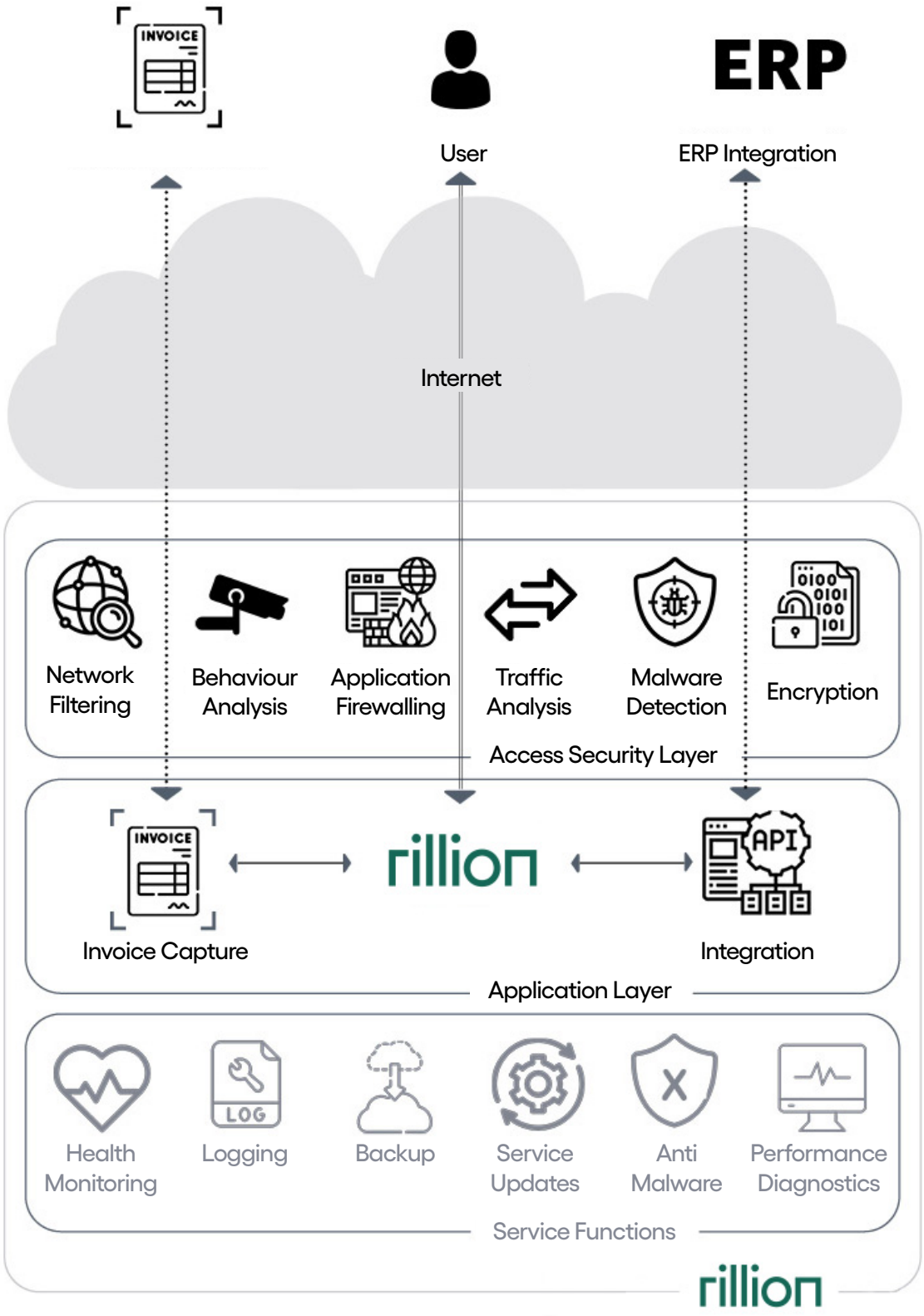
Users connect to Rillion with standard web browser over TLS encrypted HTTPS connection.

3. Integration connections

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

Besides being encrypted, Webservice access is restricted to only whitelisted known IP addresses on customer side.

Anti-Virus/Anti-Malware protection is built-in to Rillion cloud service and all data entering the platform is scanned for threats.


INVOICE
User
ERP
ERP Integration
Internet
Network Filtering
Behaviour Analysis
Application Firewalling
Traffic Analysis
Malware Detection
Encryption
Access Security Layer
INVOICE
Invoice Capture
API
Integration
Application Layer
Health Monitoring
LOG
Logging
Backup
Service Updates
Anti Malware
Performance Diagnostics
Service Functions

Authentication and Authorization

Authentication and Authorization (AA) is a business-critical factor for evaluating cloud services. Authentication is controlled through identities and roles in the Rillion cloud service which supports a strong password control.

Authorization is separated in two parts, operations and data. Rillion allocates permissions for operations and data based on roles. Each role can be used by one or several users. Each user can be part of one or several roles.

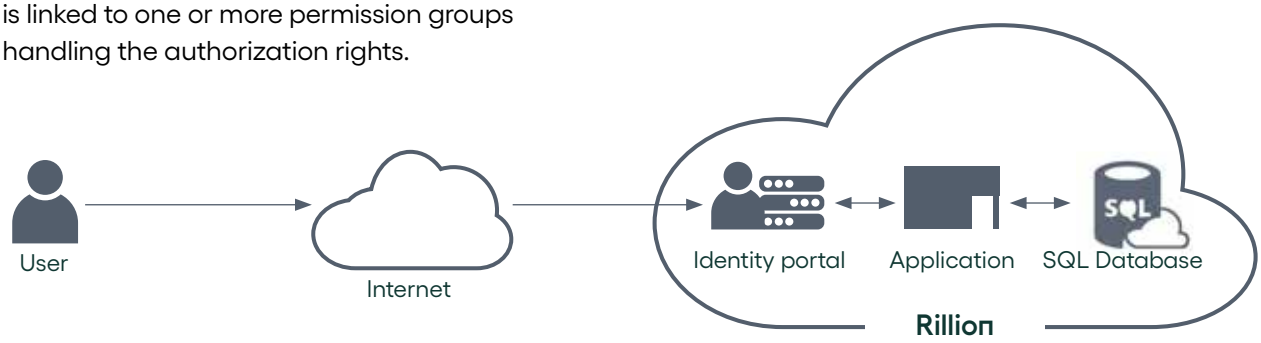
Each user in Rillion is saved as separate login account in the Rillion solution and in Identity Server portal. The Identity Server portal handles the authentication part while the authorization is handled within Rillion. Each login account is assigned to one or more roles in Rillion which is linked to one or more permission groups handling the authorization rights.

For customers

Rillion users are authenticated via Rillion Identity portal before they get access to Rillion. The user is either authenticated with internal Rillion password or via Single Sign On (SSO) services provided by external Identity providers.

For Rillion staff

Access to customer data is granted on a case-bycase basis, aka JIT access. This means that the access is time based and uses segmented AA. The principle of least privilege is used for handling internal threats.



External Identity Providers

If the customer has a public user directory service e.g. Microsoft Azure Active Directory or Google Workspace, Rillion provides customer side authentication to the resources with SSO capabilities using Open ID protocol.

Azure Active Directory (Azure AD) and Google Workspace are fully managed multi-tenant services that offers identity and access capabilities for applications running as a cloud service or for applications running in an on-premises environment.

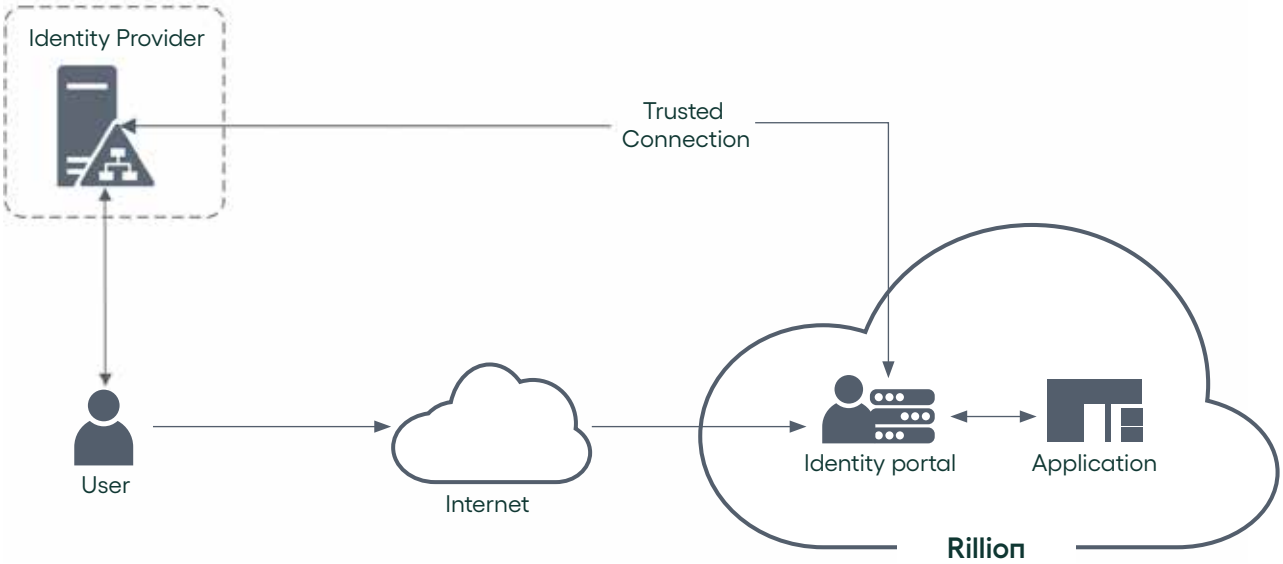
With Azure AD customers can configure single-sign on, multi-factor authentication all within their own Azure AD, making identity and access management easy and secure. Azure AD is owned and managed by the customer.

When a user logs in, the user is redirected and authenticated against the customer's own user directory as Identity Provider.

The token returned from is then used by the web browser to login to the Rillion service provided that a valid user matching the token exists in Rillion.

Rillion uses the OpenID Connect (OIDC) authentication protocol based on OAuth2 to connect to external Identity Provider.

For more details how to setup Single-Sign On using Azure AD, see articles in support portal **Freshdesk.**



Logging

Log functionality records important events and transactions and are an essential factor to providing strong security and integrity while serving as a foundation for audit trails.

Log data also provide information for identifying and troubleshooting potential problems in the platform including configuration and performance issues.

Application logging

Rillion has several different log options that can be activated for each customer specific environment. These contains information about actions and events inside the application related to normal use.

For example changes to:

- Invoices
- Flows
- Logins
- Permissions

All information logged is saved in the customer specific database.

General logging and auditing

System wide logging of events in the underlying infrastructure is done for the purpose of identifying threats and providing paper trails for audits, see the following table:

Infrastructure event	Details
Configuration changes	All connections to the platform are logged. This includes both public access as well as internal management connections from Rillion networks.
Logins	System login events, for example server level logins by Rillion personnel or database access.
Filedata modifications	All types of changes to data files, for example deletion or changes to customer data or application code.
Configuration changes	All changes to the Azure infrastructure and services.

All log information is aggregated in Microsoft Log Analytics for further processing.

Network protection

Rillion services are accessible with supported web browsers over the public Internet using the HTTPS protocol with 256-bit TLS encryption only. This means that data sent between the user and the Rillion service is always encrypted in transit.

Network security

Network security is essential for cloud services. Outside the traditional on-site network perimeter, connections are vulnerable to attacks. A high level of network security is required.

The key aspects of Rillion's approach to network security are:

1. Principle of least privilege
2. Application level firewalling
3. DDOS attack protection
4. Patch management
5. Penetration testing

1. Principle of least privilege

The internal network of Rillion is zoned and segmented with strict policies that control the traffic flow for environmental isolation and security.

2. Application level firewalling

Rillion uses an enterprise-class web application firewall (WAF) to protect the service against threats like SQL injection and cross-site scripting attacks.

The WAF service is operated in a 3rd party global vendor ecosystem allowing for automatic adaption to new threats and vulnerabilities by adding additional security layers to the traditional OWASP framework.

3. DDoS Attack Protection

Denial of Service attacks continue to grow in sophistication and force: more distributed, greater volumes of traffic, and encroaching on the application layer.

Rillion includes DDoS mitigation to maintain performance and availability of its cloud services. This includes protection against common types of DDoS attacks such as:

- DNS Flooding. By disrupting DNS resolution, a DNS flood attack will make a website, API, or web application non-performant or completely unavailable.
- UDP Amplification (Layer 3 & 4). An attacker leverages the functionality of open DNS or NTP resolvers to overwhelm a target server or network with amplified request traffic, where the payload size is greater than the size of an originating request.
- HTTP Flooding (Layer 7). HTTP flood attacks generate high volumes of HTTP, GET, or POST requests from multiple sources, targeting the application layer, causing service degradation or unavailability.

4. Patch Management

System components in the Rillion service are continuously updated for security and availability reasons by Rillion personnel as per manufacturer recommendations.

Updates are assessed when available and deployed during monthly maintenance window after successful validation in pilot environment.

5. Penetration testing

The intent of a penetration test is to simulate a real-world attack situation with a goal of identifying how far an attacker would be able to penetrate an environment.

Pen-tests are conducted on a regular basis with Manual Application Audit Testing

3rd party external audit SWAT analysts performs testing activities, identifying and exploiting vulnerabilities in as safe as possible manner to provide Rillion with an objective, third party understanding of the security level of the monitored web applications.

The SWAT continuous assessment additionally includes regular manual testing 4 times a year of the application alongside the daily assessments being conducted.

Vulnerabilities detected are escalated to Product Management for prioritization for product development.

Penetration tests are performed in accordance with the Penetration Testing Execution Standard (PTES), an industry-accepted methodology that focuses on the technical aspect of security testing. Since the standard itself does not provide any technical guidelines on how to execute an actual penetration test, additional guides are used for the target environment. Rillion uses the OWASP Testing Guide version 4.

The Testing Guide provides a checklist with common types of vulnerabilities that should be covered in the penetration test. The test methodology has been developed specifically to support the inclusion of new threats and vulnerabilities.

There are 11 subcategories of the OWASP Testing Guide Methodology that are designed to cover all types of vulnerabilities commonly affecting web applications:

- Information Gathering
- Configuration and Deployment Management Testing
- Identity Management Testing
- Authentication Testing
- Authorization Testing
- Session Management Testing
- Input Validation Testing
- Testing for Error Handling
- Testing for weak Cryptography
- Business Logic Testing
- Client Side

Customer isolation

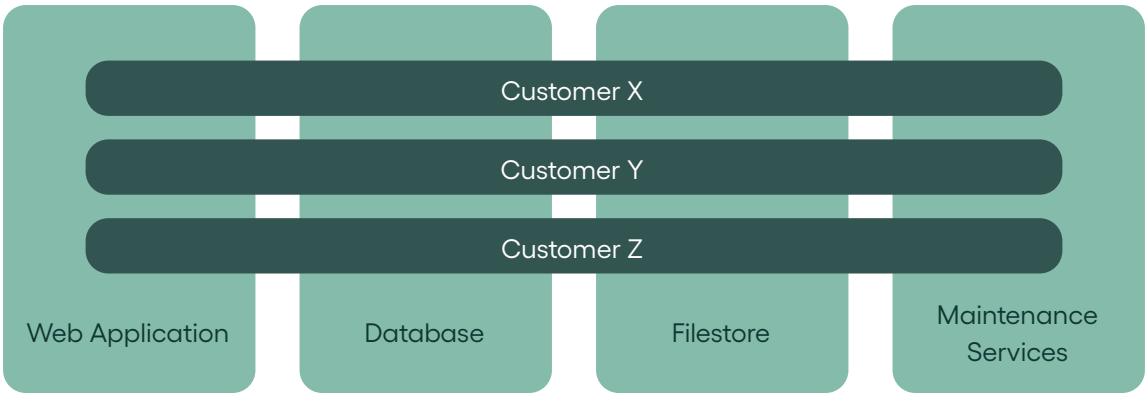
Rillion is a single tenant cloud environment. A single instance of the software and supporting services serves a single customer.

Rillion consists of several applications and supporting functions that are running in a shared infrastructure. All functionality is installed and executed on a "per-customer" basis, meaning that no customers share application code, databases or file data for the Rillion application environments.

All customer identity management below application level is centralized through Active Directory for auditing and access control. User access within the application is controlled with Security Identifiers (SID) at the database layer through SQL logins in the server engine.

The main components in the Rillion service are as illustrated below:

1. Web Application frontend
2. Database backend
3. File store
4. Maintenance Service (PAMS)



1. Web Application Frontend (IIS)

The Rillion applications runs on the frontend IIS servers in a shared infrastructure. Each customer environment within the IIS server consists of two components:

Code storage

This area contains the various application files needed to run the application and is located on the filesystem of the IIS server itself. Each customers application code is secured by filesystem ACLs restricting access to only the specific customers unique identity in the platform. No code is shared between customers.

Worker Process

This is where the application code is executed, and an isolated process is spawned using the customer unique identity for memory separation and secure access to other resources.

2. SQL Database Backend

Application data is stored in customer dedicated databases and user access is controlled through identities in the SQL server software, created and managed from within the applications. Only platform system accounts have access to multiple databases, customer specific identities are restricted to related databases only.

3. File Storage

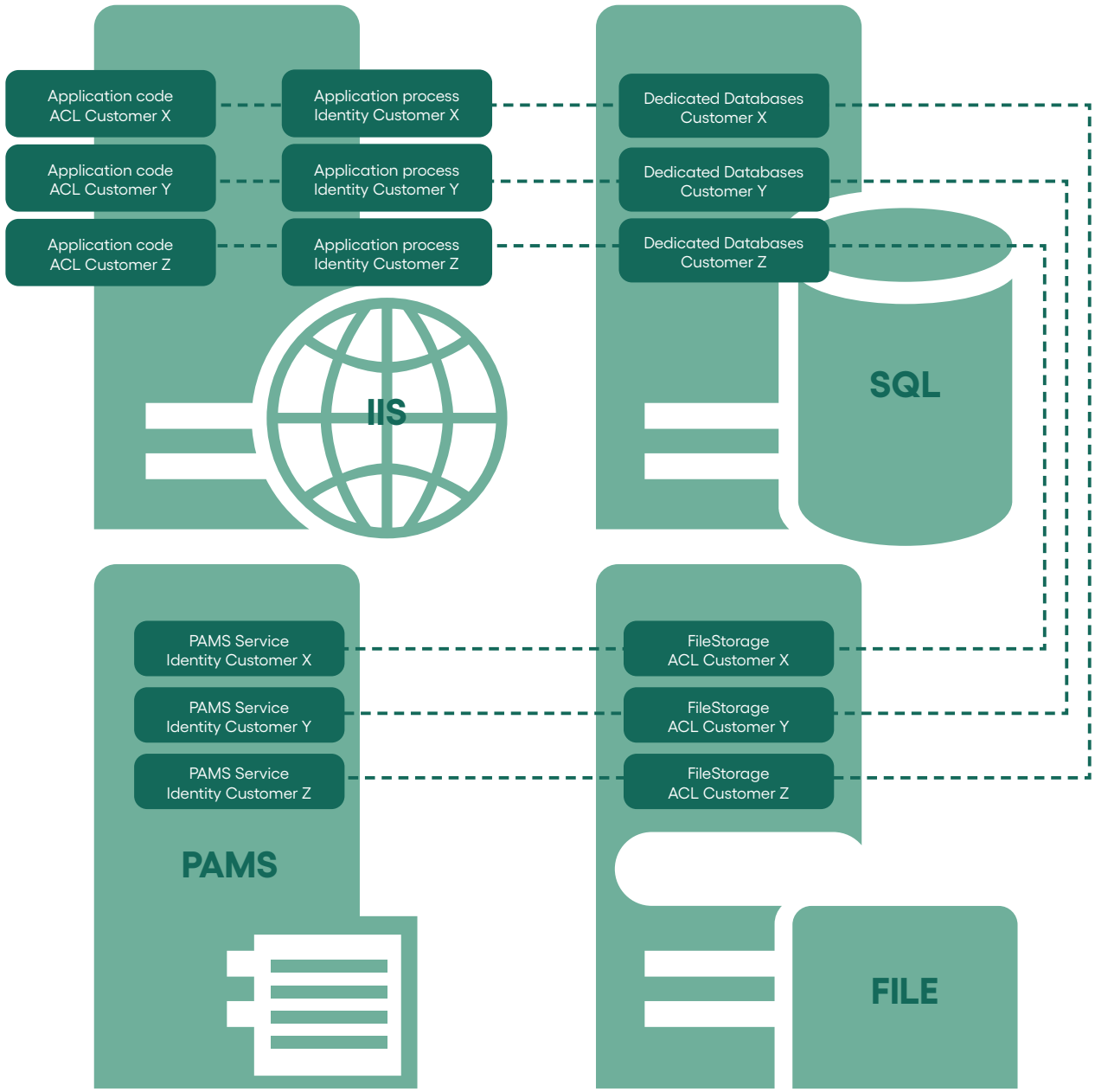
File-based customer data is stored on separate server resources and customer isolation is maintained through filesystem ACL restrictions. Only the customer specific platform identity has access to customer data in addition to system level accounts.

No databases containing customer data are shared between customers.

4. Rillion Maintenance Service (PAMS)

The Rillion maintenance service is a per-customer application running as a windows service on shared server resources. The service process is executed under the same unique customer identity as the web application which ensures that only access to customer specific resources is permitted, such as file storage.

Customer environments in the shared infrastructure is completely separated across all resources and server functions. The use of ACLs and dedicated process identities ensures that only access to relevant data is permitted.


Application code
ACL Customer X
Application code
ACL Customer Y
Application code
ACL Customer Z
Application process
Identity Customer X
Application process
Identity Customer Y
Application process
Identity Customer Z
IIS
Dedicated Databases
Customer X
Dedicated Databases
Customer Y
Dedicated Databases
Customer Z
SQL
PAMS Service
Identity Customer X
PAMS Service
Identity Customer Y
PAMS Service
Identity Customer Z
PAMS
FileStorage
ACL Customer X
FileStorage
ACL Customer Y
FileStorage
ACL Customer Z
FILE

Physical security

All data stored in Rillion is located in Microsoft Azure datacentres. Microsoft designs, builds, and operates datacentres 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 datacenter resources. Datacentres 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 datacenter floor.

Physical security reviews are conducted periodically of the facilities to ensure the datacentres 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 rillion.com broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1, SOC 2 as well as country- or region-specific standards, including Australia IRAP, UK G-Cloud, and Singapore MTCS. Rillion servise organisation is examined for SOC2.

Rillion EMEA services are primarily delivered from the Microsoft Netherlands datacentre (West Europe Region) with secondary backup functionality in the Ireland datacentre (North Europe Region). Customer data is therefore never stored outside the EU region.

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 Rillion code base, Rillion technicians offer the best possible service and support for the cloud services and delivers agile and responsive development of new releases.

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

AP automation with Palette 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