cunesoft
compliance delivered

High Security SaaS Concept

Software as a Service (SaaS) for Life Science

© Copyright Cunesoft GmbH

Contents

Introduction

IT Budgets are being more and more limited in today's business world. In order to save costs, most companies consider implementing a cloud based or Software as a Service (SaaS) solution, in order to cut total cost of ownership.

Main question being asked, and not only from Data Security Officers, is "how can such a system be provided as secure as an on premise installation, respectively can it be implemented even more secure?"

The following whitepaper provides a detailed view into the Cunesoft private cloud architecture and describes how an end-to-end security is being achieved. Furthermore the promise is that the reader will find many aspects of exceeded security over currently and commonly used on premises architecture.

This whitepaper will focus on how the following security aspects are being ensured and fulfilled:

- Data Security on Cloud Storage Systems
- Data Isolation on Cloud Storage Systems
- Data Integrity
- Backup / Recovery in the Cloud
- Application Level Security
- Transport Level Security

Data Security and Isolation in the Cloud

Storage System Security and Isolation

The foundation of each computer system is the storage system, at which all data, all configurations and all knowledge is persisted. Securing this system is the first part to a secure private cloud environment.

The Cunesoft implementation is based on encryption alongside with separation. Each customer in the Cunesoft private cloud is being assigned an individual database, an individual storage drive, as well as a unique encryption key.

The separation of storage drives ensures that a customer only has access to the data specific to his implementation and data set. This layer ensures that customer's data is always separated from other customer's data and via that secures each customers bucket of data.

After separation of each data bucket is ensured, another layer of security has been added to ensure that the customer itself can only access the data stored within the bucket and that the data is secure even in an event of physical access to the server, due to maintenance or other events. Data encryption for each data bucket ensures this additional security.
Each customer is provided with an individual, unique encryption key. This key is then used by the application layer (user interface) to encrypt all data that is passed into the system before being stored on a server. Upon data read the data is transferred from the storage bucket, decrypted again on the application layer and then displayed to the user – ensuring that no unencrypted, insecure data is stored on any server at any time.

Database Security and Isolation

Data security for files stored on servers is one part of data security. Another important component of information is not stored on servers but in database systems, such as records and audit trails.

Cunesoft is using Microsoft SQL Server as a storage engine. The database engine supports multiple databases as well as a transparent data encryption.

Each customer instance within the Cunesoft private cloud is provided with a completely separate database automatically and alongside with an individual user account, used to connect the application Layer to the database Layer.

Sensitive data is then automatically encrypted, once written to the database.

User Identity and Access Management

User de-provisioning is an issue that will become more challenging as password-authentication methods grow in complexity and volume. Federated identity management schemes will make it easier for users to log on to multiple clouds, and that will make de-provisioning much trickier. Typically IT departments wish to have a process and routine defined, that describes and ensures that when an employee leaves the company, this person gets de-provisioned from their Windows account and any internal enterprise applications, their mobile phone gets wiped of corporate information, and they're blocked from the company's SaaS applications.

Cunesoft fulfills the user identity, access management and de-provisioning in the following manner:

- Each user is identified by a unique username by the system.
- Each user initially receives an automatically generated password, which can be changed by the user at any time.
- Administrators can generate a new password for each user assigned to them, however no administrative user can see or access the password assigned to a user.
- Password policies can be enforced, forcing a certain complexity within a password or forcing the user to change the password on a specified schedule.

Data Integrity

All data, regardless if the data is stored on servers or disk drives, or if the data is stored within the database system, is stored on a disk array with multi disk configuration. This ensures that even if a disk within the array fails, all data is still available online.

Another layer of security is mirroring. Data is automatically mirrored to different data centers, ensuring that every piece of information stored within the cloud is still available, even if the primary datacenter is completely disconnected or destroyed in case of a disaster.

The mirrored data center is ensured to be in a different country, to ensure data security and availability even in the worst-case scenarios. Data mirroring is an automated process that is replicating the data written to disk, database and the complete server environment to the fall back datacenter upon write request, ensuring data integrity at all times.

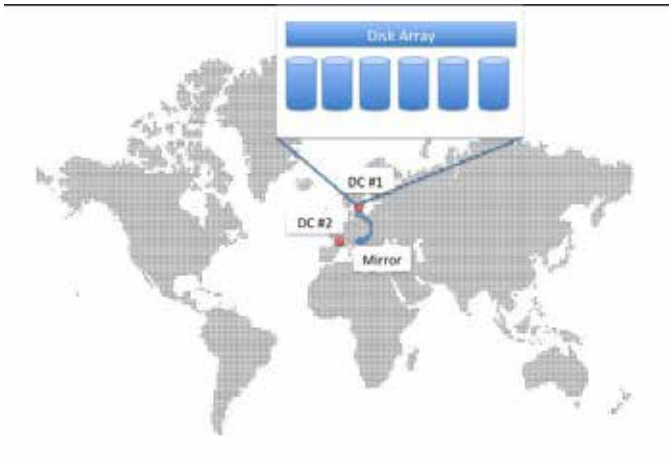
All data centers used by Cunesoft to operate, guarantee an uptime of min. 99 % - Cunesoft guarantee's the same level of availability with the exception of scheduled

update days, where new versions of the Cunesoft cloud are populated within the environment. This maintenance window is communicated well in advance and scheduled during low peak times. The overall availability during patching and upgrade windows is 99%.

Location & Performance

Cunesoft's data centers are all European based data centers for our European customers to ensure the highest performance possible within Europe. However, cloud based solutions have the benefit of being decentralized. This means that the application implemented within the Cunesoft cloud might be accessed from other places scattered around the world.

To ensure the highest performance possible for all end-users worldwide, Cunesoft offers an optional content delivery network service. This Service ensures that data is delivered from a connection point near the end-user, transferring the data to that point within the optimized delivery network. This provides the user with high bandwidth, low latency and fast access times across the globe.



Another optional service is the analysis and optimization of the customer's network. Essentially, data that is stored in the cloud needs to be transferred over the Internet from and to the client's network to work and / or display the data. For a fast and reliable connection and high user acceptance and satisfaction it is important to ensure connectivity at the highest bandwidth possible. One possibility to optimize the network to and from the Cunesoft cloud is implementing caching facilities such as Riverbed technologies and WAN optimization.

European Data Security Act

The European Union recently submitted a guideline for member states to update data security and data protection laws. The new laws enforced by the member states caused a lot of confusion especially in the Cloud Segment of Information Technology.

At the heart of all laws passed within the member states, the data security act requires to ensure the following:

- The command and control of data lies with the customer and is not controlled by anyone outside
- Customers must be able to safely delete data
- An audit trail must be available documenting all manipulated data details

Cunesoft addresses all of these requirements in its high security cloud concept. Due to the nature of Part 11 Compliance, the requirement of having an audit trail is fulfilled. Deletion of data is possible within the cloud implementation and is ensured by automated checks within the cloud implementation.

Cunesoft documents all details on datacenter location hosting and documents which data centers it is being mirrored too. This ensures that customers have control over the location of their data and know where it is stored at all times.

Backup and Recovery

The Cunesoft private cloud supports two backup and recovery models.

Cloud Based Backup and Recovery

The cloud based backup and recovery service will be an automated service, which transfers all data to a secure storage area network in two data centers across the globe.

Based on a defined schedule, all files, databases and system installations are packaged automatically, encrypted and stored in two different locations in the cloud, to ensure maximum data security.

The guaranteed backup time by Cunesoft is six to eight hours, depending on the size of data restored.

Traditional Backup and Recovery

The second model is a traditional backup and recovery model, which can be implemented in following the customers on premise back up strategy. The Cunesoft private cloud provides a file share, where all data is being exported too, based on a defined schedule. The customers backup and recovery solution will be able to pick up the data from the file share.

Via this alternative backup and recovery option, customers can continuously store a copy of all relevant data within their organization and keep a copy at all times. Upon request, the data provided on the file share can be decrypted, or a tool to decrypt the data will be provided by Cunesoft, so that even on premise, the data is stored in a high security manner.

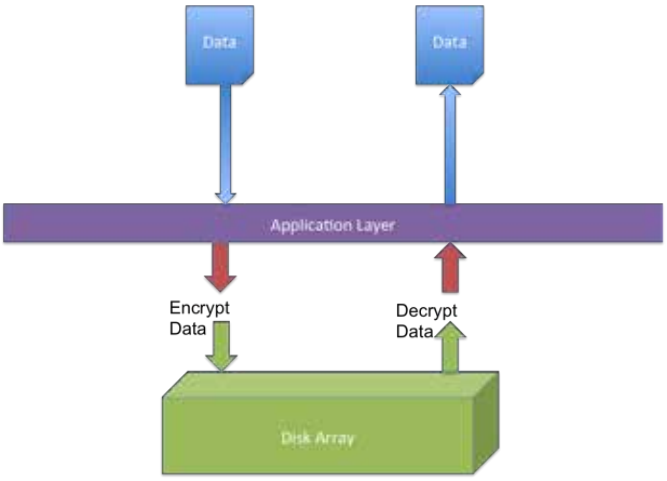
Application Layer Security

The front end application layer, in essence the real application, is the consolidated user interface for customers, which combines all components discussed and described in previous sections of this whitepaper.

Each time a user uploads or creates a piece of information within the system, the application layer ensures that all data, documents and other information is being stored to the appropriate and correct databases and storage buckets within the Cunesoft high security private cloud environment.

Before storing files on any storage environment, the application layer routine automatically encrypts all data with the unique customer key, to ensure that no human readable data is stored within the cloud storage systems at any time.

Upon access to information for download or read, the application layer retrieves the encrypted piece of data, transfers it into memory, decrypts it and displays it to the user. This is being done with applied transport level security, ensuring that even if a user requests data, there is no piece of information stored unencrypted within the system.

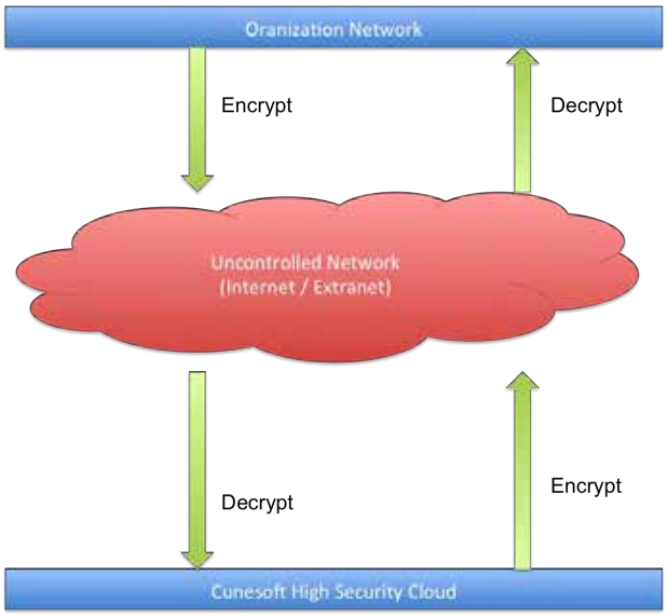


Another service offered by the application layer provides authentication and authorization. Whenever a user accesses the Cunesoft system, the user is prompted for a username and password. This unique combination ensures that the user is directed to the specific customer's accounts and corresponding data buckets for this specific account. For further details, refer to the previous chapter data security and isolation of this whitepaper.

Once authenticated, the system proceeds to the authorization stage, as with any non-cloud based document and data storage environment. The authentication and authorization is completely transparent to the underlying system.

Transport Level Security

As with all cloud based systems users connect to this environment through the Internet. The connection from the customer's network to the cloud environment is always made through the Internet, regardless of the connection type: HTTP or VPN, all connections have to go through the public internet in order to make a successful connection.



The key aspect to consider for connections through the internet is to ensure that all data flowing in and out is encrypted and secured at all times, especially in the case of transferring user data such as username and password.

To force this security rule, Cunesoft allows encrypted HTTP connections through HTTPS only. Users are automatically redirected to the secure connections, even if the attempt is made to establish an unsecured connection. The User and all accessing software, such as browsers, are forced into a secure channel before any data is transferred between the cloud and the end user. This security measure is also enforced, in case any download or upload happens.

Conclusions

Creating a high security cloud implementation requires a thorough detailed concept and execution on a "rock solid" application architecture and infrastructure.

Even if a cloud service is not connected through VPN networks, highest levels of security are reached with the Cunesoft implementation and architecture concept. Encrypting data end-to-end should provide complete confidence on securing that only authenticated users are able to read data. Data separation ensures that encrypted data cannot be accessed by anyone outside the organization.

The HTTPS encryption closes the gap between the cloud service and the corporate network to ensure that the data flowing between these services cannot be accessed unencrypted. Implementing data mirroring between data centers and redundant backup and recovery facilities ensures that our customers data is available and accessible at all times – even in case of a disaster happening in the primary hosting data center.

Contact us for a Live Demo

Cunesoft GmbH
Luise-Ullrich-Strasse 20
80636 Munich
Germany
Phone: +49-(0)89-235 14741
Website: www.cunesoft.com
E-mail: info@cunesoft.com