eppendorf

WHITE PAPER No. 67

# Security Measures Supporting VisioNize® Lab Suite


## Introduction

The laboratory has always been a truly interconnected place – not just because of the equipment and collaborations going on, but also because of the constantly evolving links between different scientific disciplines, views, and cultures. And the role of cloud-based working in all of this is to make connectivity easier and more reliable!

Not long ago, security concerns were a reason for people and companies to be hesitant to use and trust cloud-based services. Nowadays, security is one of the main reasons for migrations into the cloud. The rationale behind this migration is the superior ability of large public cloud service providers to protect applications and the data of cloud-based assets.

Protecting the data of our customers while offering cloud-based services is of the highest priority for us at Eppendorf. Therefore, we have implemented several standards and policies that support the security of VisioNize Lab Suite (VNLS) and prevent unauthorized access to it. This affects data storage and housing of our VisioNize Lab Suite service applications – e.g., Alert+ and Task Management. This document describes the various standards, data security approaches, business practices, and certifications used for the cloud-based storage that supports VNLS and its services.

## Security architecture

Our digital platform VisioNize Lab Suite is designed with lab security as the driving force – from the infrastructure to the application levels.

Some central components of VisioNize Lab Suite, such as device connectivity, user management and audit trail, are built on Software AG's Cumulocity IoT platform[1] and hosted for Eppendorf on Microsoft® Azure®. This guarantees platform compatibility with additional Eppendorf cloud-based services hosted on Microsoft Azure that are part of VisioNize Lab Suite. Other apps of VisioNize Lab Suite, for instance,

those used for long-term storage of data and experiment management, are developed and operated by Eppendorf in a separate Microsoft Azure environment. The list of such apps will grow in the future, and their development and operation will be conducted under the same governance principles as outlined below in this paper.

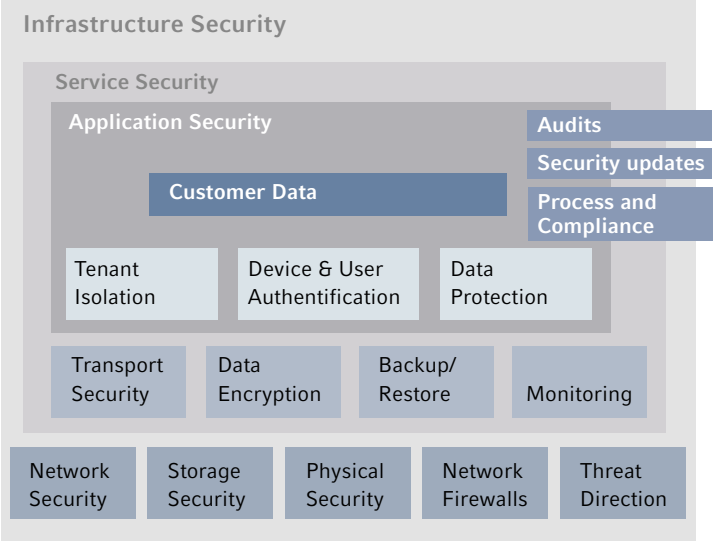


**Figure 1:** Architecture supporting the VisioNize Lab Suite

VisioNize Lab Suite uses a three-layer security model, providing infrastructure, service and application security. Infrastructure and service security is provided by Software AG's Cumulocity IoT platform and the security architecture of Microsoft Azure. Application security is provided by design and the specific implementation of tenant isolation, device and user authentication, and data protection.

The security of VisioNize Lab Suite, including its interfaces with external systems and connected devices, is provided for data during transit and at rest, access control and authorization, and, specifically, GDPR compliance. The same design guidelines apply to the device software, which can be downloaded from VisioNize Lab Suite to the device.

Audits, security updates, and processes extend through all layers to ensure end-to-end lab security.

## Data at rest

Data at rest means all data that is persistently stored within the VisioNize Lab Suite. Such data is encrypted using a 256-bit AES encryption, compliant with FIPS 140-2. All Azure storage redundancy options also support encryption, and all copies of a storage account are encrypted.

VisioNize Lab Suite implements multitenancy so that the data of one customer is separated from all other customer's data, and only users of that customer have access to the customer's data to the extent their role and related permissions in VisioNize Lab Suite allow them.

All data is stored solely in the VisioNize Lab Suite database. This includes user data (the names and email addresses as provided by the customer's tenant administrator[s] and phone numbers provided by your users – optional if notifications via SMS are setup) and device data (serial numbers of the devices and the attributes set by your users – e.g., location). It also includes performance data like events and measurements; runtime and maintenance data like calibration status, user-defined configurations, and settings (e.g., notification settings and maintenance reminders); audit-trail information, including device and software usage; and experimental protocols and documentation of experiments, including used protocols, executing person, used devices, and annotations.

Some types of data are always stored independently from the services subscribed to by the individual customer and are only accessible to the individual customer if he or she has subscribed to the related service during the subscription process. This applies, for instance, to the audit-trail data that logs device events and when a user logs on or off. This requires the VisioNize Lab Suite service Device Documentation. After subscribing to Device Documentation, customers will also have access to audit-trail data that was generated before the subscription started.

## Data in transit

Data in transit – i.e., all data being transferred between a device and the cloud or other services and the cloud – is secured by TLS/HTTPS, which ensures full encryption of all transferred data. This applies to all data that devices send to the cloud and data sent from the cloud to devices – e.g., for devices in cases where a VisioNize Lab Suite user remotely defines certain attributes like nickname, location, maintenance tasks, and configuration of a device. VisioNize Lab Suite does not allow devices to be controlled remotely.

## Authentication

Authentication of users in VisioNize Lab Suite is performed via the OAuth2 internal log-on mode of Cumulocity. OAuth2 is a widely used standard for secure web-based user authentication. Devices are registered by their owners and VisioNize Lab Suite users who have permission to register devices.

## Authorization

The intention of VisioNize Lab Suite is for each user to utilize his or her own individual account. An extensible user-role concept provides each user with the required permissions according to the roles assigned by the customer's administrator of VisioNize Lab Suite in the laboratory environment. VisioNize Lab Suite provides an intuitive and lean role and permission model that distinguishes between a reasonable and manageable number of roles with associated permission sets.

As stated in the Eppendorf terms and conditions, personal client data will only be processed for the purpose of providing the service (e.g., creation of the tenant, notification in case of service disruption). Eppendorf may anonymize or aggregate device and software performance data for the purpose of improving current services and devices or to develop new services. Eppendorf will not access measurements on samples, scientific results, protocols, experiments, and workflows.

Upon request by Eppendorf Product Support, a customer's user with administration permission can create a user with a separate role that grants a member of Eppendorf Product Support (temporary) access to the customer's tenant for troubleshooting purposes.

For administrative access, VisioNize Lab Suite maintains a standard release and change management process that is reviewed by key stakeholders, including Eppendorf Quality Assurance and Release Management. Least access privileges are assigned, and administrators only have access to the specific infrastructure and services necessary to deploy new versions of the VisioNize Lab Suite application; they do not have access to the customer's data.

## GDPR

To give you full control over all your personal data in VisioNize Lab Suite, all acquisition, processing, and storage of personal data are fully compliant with General Data Protection Regulation (EU) 2016/679.

## Security updates and disaster recovery

Security updates to the VisioNize Lab Suite and the software on devices are provided at an accelerated pace and independently from the release cycle of new software versions. The system utilizes open source components, which are stable and tested to build on security-proven components where reasonable.

All stored data is backed up by automatic backup procedures in regular intervals and with reasonable retention periods as required by the criticality of the different types of data.

## Security audits

Development of VisioNize Lab Suite follows the agile development paradigm and includes several activities to design and test for security. Adoption of agile principles into software development leads to shorter software release cycles plus early and continuous integration of customer feedback into software development. This increases flexibility regarding requirements and improves the resulting quality. Continuous verification of the software facilitates quick detection of and response to any unintended behavior or defects.

External partners specialized in the field of IT security assessment and testing are involved in development and support; they provide design reviews and extensive testing of the security infrastructure, including penetration testing to ensure security is an inherent part of the development process of VisioNize Lab Suite and included by design.

## Incident management

Eppendorf and its suppliers have implemented processes for corrective and preventive actions (CAPA) as part of their quality management systems. These processes include procedures for reporting, tracking, resolving, and communicating security incidents and their related corrective and preventive measures.

## Acronyms

AES: Advanced Encryption Standard
API: Application Programming Interface
DoS: Denial of Service
FIPS: Federal Information Processing Standards
GDPR: General Data Protection Regulation
HTTPS: Hypertext Transfer Protocol Secure
IoT: Internet of Things
TLS: Transport Layer Security
OAuth: Open Authorization (protocol that allows a standardized, secure API authorization for desktop, web and mobile applications)

## References

1. Software AG, "Securing your business on the Internet of Things" (white paper, 2020), https://resources.softwareag.com/products-analytics-decisions/2020-7-wp-cumulocity-iot-security-en-white-paper.

## About Eppendorf

Eppendorf is a leading life science company that develops and sells instruments, consumables, and services for liquid-, sample-, and cell handling in laboratories worldwide. Its product range includes pipettes and automated pipetting systems, dispensers, centrifuges, mixers, spectrometers, and DNA amplification equipment as well as ultra-low temperature freezers, fermentors, bioreactors, $CO_2$ incubators, shakers, and cell manipulation systems. Associated consumables like pipette tips, test tubes, microtiter plates, and disposable bioreactors complement the instruments for highest quality workflow solutions.

Eppendorf was founded in Hamburg, Germany in 1945 and has more than 4,800 employees worldwide. The company has subsidiaries in 30 countries and is represented in all other markets by distributors.

## More Information

If you would like to learn more about VisioNize and its benefits for You and Your Lab, please visit our website: **www.eppendorf.com/visionize**

**Your local distributor: www.eppendorf.com/contact**
Eppendorf SE · 22331 Hamburg · Germany
eppendorf@eppendorf.com · www.eppendorf.com

www.eppendorf.com

Microsoft® and Azure® are trademarks of the Microsoft Cooperation, USA.
Eppendorf®, Eppendorf Brand Design, VisioNize® and the VisioNize logo are registered trademarks of Eppendorf SE, Hamburg, Germany.
All rights reserved, including graphics and images. Copyright © 2021 by Eppendorf SE, Hamburg, Germany. Eppendorf SE reserves the right to modify its products and services at any time. This white paper is subject to change without notice. Although prepared to ensure accuracy, Eppendorf SE assumes no liability for errors, or for any damages resulting from the application or use of this information. Viewing the white paper alone cannot as such provide for or replace reading and respecting the current version of the operating manual.