WHITE PAPER No. 55

Security Measures Supporting VisioNize Digital Lab Space

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.

Introduction

Protecting the data of our customer while offering cloud-based services is of the highest priority for us at Eppendorf. Therefore, we have implemented several standards and policies supporting the security of and preventing unauthorized access into the VisioNize Digital Lab Space used for data storage and housing of our VisioNize service apps.

This document describes the various standards, data security approaches, business practices, and certifications used for the cloud-based storage that supports VisioNize and its services.

Network architecture

Our digital platform VisioNize is designed with security as the driving force – from the infrastructure to the application level.
Our Digital Lab Space relies on the Microsoft® Azure® infrastructure, taking advantage of its wide array of security tools, capabilities, and its guaranteed 24/7 availability of services.

VisioNize contains several security layers to protect customer data from unauthorized access or manipulation.

The security of VisioNize applications is built upon a strong foundation of secured Azure services and infrastructure. Audits, security updates and processes reach over all layers to ensure end-to-end security. The servers utilized for the Digital Lab Space are located in the EU and all data are stored on servers within the EU.

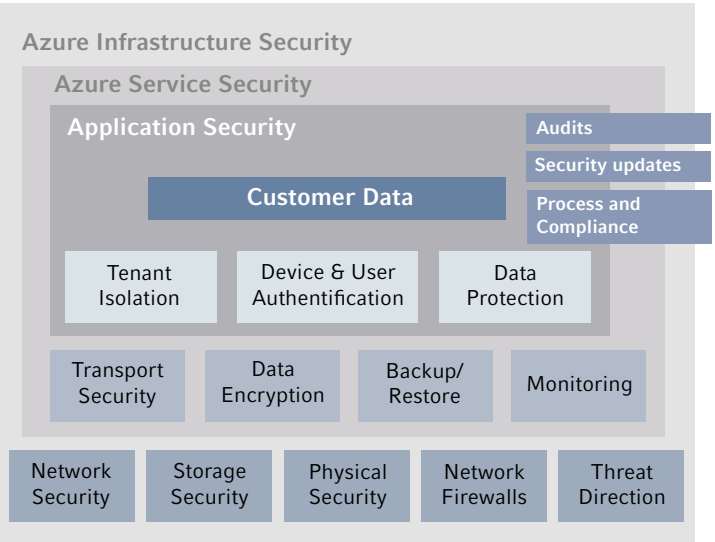

Figure 1: Architecture supporting the VisioNize Digital Lab Space

Platform and network and security

Security is an inherent part of the development process of VisioNize. Therefore, several security mechanisms already provide protection on a network level, such as protection against so-called "distributed denial-of-service (DoS) attacks". Those attacks are geared towards making a machine or network resource unavailable by flooding the targeted machine or resources with superfluous requests. The attempt is to overload systems and prevent some or all legitimate requests from being fulfilled.

Built-in firewalls control the access to network resources of the Digital Lab Space to deliver sufficient protection against unauthorized access.

Incident management

The Azure Security Center is used for constant assessment of the implemented protection measures and immediately implements recommended measures to increase the security of the system to current technical standards.

The Azure Advanced Threat Detection is enabled to provide real-time notifications. In the unlikely event that a threat has been detected by Azure threat monitoring, the threat will be assessed immediately and adequate actions will be taken. If a condition appears where customer data or the provided services should be affected, Eppendorf will notify customers immediately and carry out an investigation to determine all possible causes.

Data storage

All data are stored in the Digital Lab Space. The data VisioNize and its services are storing include:

> **User data:** provided names, email addresses, and telephone data for receiving VisioNize notifications
> **Device data:** serial numbers of the connected devices, as well as performance data like door openings, runtime, etc.

Access Control

Authentication
Authentication of users in the Digital Lab Space is performed via an Open ID Connect protocol, which is a widely-used standard for web-based user authentication. An extensible user role concept provides each user with the required permissions according to the assigned roles by the administrator of VisioNize in the laboratory environment.

All communication from devices is secured with individual device certificates. Each request to the servers of the Digital Lab Space is secured with server certificates, routing back to a trusted certificate authority.

Each communication request requires a successful server authentication plus a user and / or device authentication to provide the highest possible degree of security. Furthermore, it prevents any unauthorized third parties to read, modify, or deny access to data without authorization.

Encryption
With the Digital Lab Space, all data is handled with the utmost care to prevent any unauthorized access. This includes a state-of-the-art approach to data encryption. Here are the two types of encryption methods used:

In transit
Data in transit means all data that is transferred between your devices and the cloud is secured by Transport Layer Security (TLS/HTTPS) that ensures full encryption of all transferred data.

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

Updates
Security updates to the Digital Lab Space are provided at an accelerated pace and independent from the release cycle of new software versions. The system utilizes open source components which are stable and tested to build upon security proven components where reasonable.

Backups
All data stored, meaning user account details like email address and names, as well as device information in form of serial numbers, are backed up automatically with Azure Managed Backup in daily, weekly, and monthly intervals, and can be restored by Eppendorf in case of failure. Events that devices have sent to VisioNize are stored in a master database and replicated into geo-redundant secondary databases on a geo-redundant storage of Azure.

Authorization
The intention of VisioNize is for each user to utilize his or her own individual account. For administrative access, Eppendorf maintains two-factor authentication; logins with the highest permission levels trigger alarms that are monitored by the CIS team.

For administrative access, it is maintained and audited for appropriateness. VisioNize maintains a standard change management process that is reviewed by key stakeholders including QA and Release Management. Least-access privileges are assigned, and administrators only have access to specific infrastructure and services that are necessary to provide support to their microservices.

GPDR

To give you full control over all your personal data in VisioNize, all acquisition, processing, and storage of personal data is fully compliant to the General Data Protection Regulation (EU) 2016/679 (GDPR).

Software development

The development of the VisioNize follows the agile development paradigm. Adoption of the agile principles into software development leads to shorter release cycles of the software plus early and continuous integration of customer feedback into software development. This increases the flexibility regarding requirements and improves the resulting quality. Continuous verification of the software facilitates a quick detection and response to any unintended behavior or defects.

External partners who are specialized in the field of software security are additionally involved in the development and support with design reviews and extensive testing of the security infrastructure, including penetration testing, to ensure that security is an inherent part of the development process of VisioNize and included by design.

Acronyms

CIS	**Continuous Improvement Software**
DoS	Denial-of-service
FIPS	Federal Information Processing Standard
GDPR	General Data Protection Regulation
HTTPS	Hypertext Transfer Protocol Secure
TLS	Transport Layer Security
QA	Quality Assurance

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

About Eppendorf

Since 1945, the Eppendorf brand has been synonymous with customer-oriented processes and innovative products, such as laboratory devices and consumables for liquid handling, cell handling and sample handling. Today, Eppendorf and its more than 3,000 employees serve as experts and advisors, using their unique knowledge and experience to support laboratories and research institutions around the world. The foundation of the company's expertise is its focus on its customers. Eppendorf's exchange of ideas with its customers results in comprehensive solutions that in turn become industry standards. Eppendorf will continue on this path in the future, true to the standard set by the company's founders: that of sustainably improving people's living conditions.

Your local distributor: www.eppendorf.com/contact
Eppendorf AG · Barkhausenweg 1 · 22339 Hamburg · Germany
E-mail: eppendorf@eppendorf.com

www.eppendorf.com