eschbach

# SECURE YOUR SOFTWARE WITH SHIFTCONNECTOR® CLOUD

www.shiftconnector.com

ISO 9001 QUALITY MANAGEMENT

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

# TABLE OF CONTENTS

# INTRODUCTION

**eschbach has developed Shiftconnector®, an enterprise software platform for the process management of chemical and pharmaceutical production plants.** Shiftconnector® is used worldwide by leading companies such as Bayer, DuPont, BASF and Roche.

Since 2005, available as an on-premise solution only, eschbach adapted to the increasing demand for cloud offerings and has offered Shiftconnector as a software-as-a-service since 2015. Data security is the highest priority at eschbach and its information security management system is certified according to ISO 27001. In addition, its quality management system is certified according to ISO 9001. This ensures that procedures, like a comprehensive access control and change management, are in place to secure our Shiftconnector cloud.

This paper outlines the security measures eschbach implements to ensure the confidentially, integrity and availability of its cloud systems and data.

# SECURE ARCHITECTURE

## Infrastructure

To ensure a high level of availability and stability, the Software-as-a-Service solution is operated in a dedicated virtual cloud. Customers can choose either our Newark, NJ, location in the U.S. or our Frankfurt, Germany location. For the U.S. data-center, there is a SOC 2 report available and both U.S. and Germany datacenters have an ISO 27001 certificate.

Access to the cloud systems and applications is secured by multiple layers of firewalls and the servers are configured to only allow necessary ports. IP whitelisting to restrict access to customer resources is available.

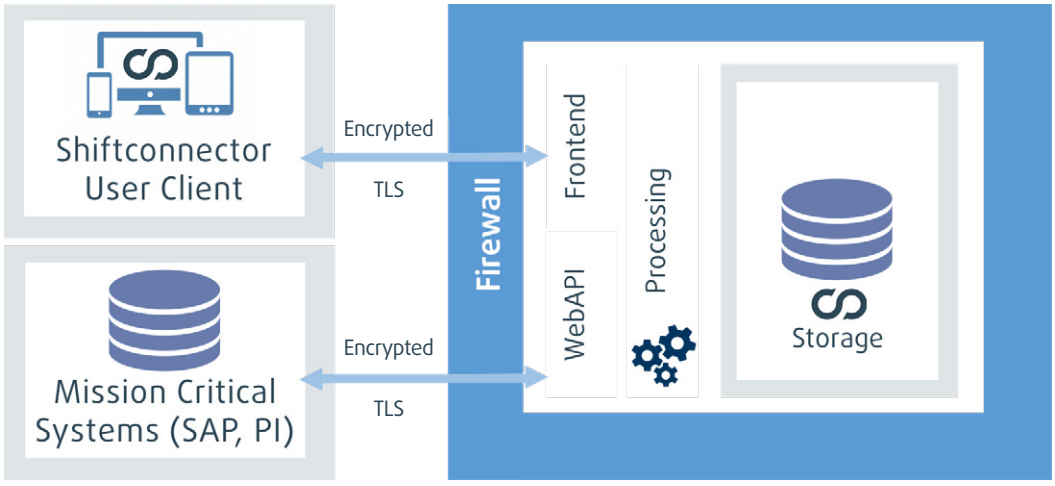
Only HTTPS is used for communication between the Software-as-a-Service solution and external services. This is enforced both at the server level and at the application level.

## Software

In addition to infrastructure security, software security also plays a central role. For the development and operation of Shiftconnector, eschbach follows a secure product lifecycle.

Security measures play a major role, from requirements gathering through to deployment and decommissioning of a release. These measures include topics such as the use of security champions, security code reviews, automated security analyses, a secure build process, and much more. Critical values, such as the application settings or the authorization tokens for the mobile Shiftconnector GO app are stored encrypted.

The application has a multi-tenant architecture with integrated and extensible authorization roles. For authentication and authorization, Shiftconnector supports many established identity providers like OpenIDConnect, on which Azure AD is based.




Secure Cloud Infrastructure

# BACKUP AND DISASTER RECOVERY

Availability is one of the core components of security. This includes the availability of the application and the underlying data. Especially in case of a data loss, the availability and integrity of backed up data is crucial.

To fulfill this availability, eschbach utilizes geo redundant servers and database backups. Starting from time intervals of up to a few hours up to several months, these backups undergo documented backup and restore tests to ensure the functionality.

Procedures for dealing with disasters and interruptions to business continuity also are in place. Disaster recovery and business continuity plans are available as part of the ISO 27001 certified information security management system.

# MONITORING

Our security monitoring is based on information gathered from the internal networks, servers, application data, configuration data and open-source information. For the internal network and the cloud servers, eschbach monitors various metrics to determine the availability, health and security of its systems. Additional endpoint protection solutions and monitoring programs are in place to check the configuration of the cloud offering for misconfigurations, which could lead to a vulnerability.

In addition, threat intelligence is gathered with honeypots and open-source information. Systems are checked against public databases of reported IPs that are involved in malicious activity. This provides an additional layer of security as it relies not only on internal data, but also on external data.

Regular monitoring of identity leakages related to our cloud domains are performed to find customer accounts which were breached through a third party. For example, malware may infect a personal computer, which then steals and publishes login credentials related to our domain. We look for published datasets related to our SaaS-domains to identify external breaches that could affect our cloud security.

There is a dedicated eschbach team who is responsible for monitoring and analyzing, and in the case of an alert, multiple messaging channels are in place to ensure that customers are notified.

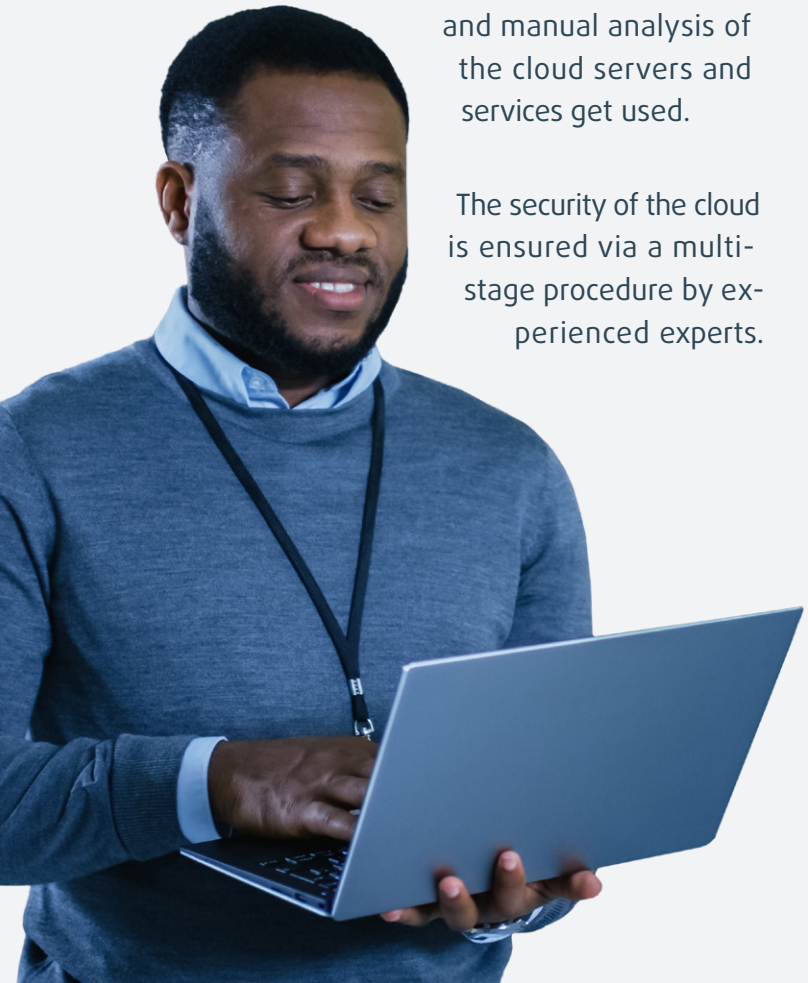
# TESTING AND ANALYSES

Regular testing and analysis of the infrastructure and the hosted application is crucial. Our eschbach security team collaborates with external companies, like the DCSO[1], to carry out multiple analyses on different layers of its infrastructure.

## Infrastructure

The eschbach cloud infrastructure and its (web-) servers are analyzed annually. TÜV Rheinland[2] conducted an external penetration test in 2021 and 2022 (please find further details here). The analysis includes a black-box approach, which performs the analysis from "the outside", like an attacker would do. Well-known standards represent an important part of the analysis. Both automated and manual analysis of the cloud servers and services get used.

The security of the cloud is ensured via a multi-stage procedure by experienced experts.



The cloud infrastructure also is analyzed from the inside by compromised assessments. The goal of this is to find traces of current and past attacks in the system and network. This is particularly relevant regarding advanced persistent threats. For the compromise assessments, eschbach collaborates with the DCSO.

## Software

TÜV Rheinland conducted a penetration test for the cloud instance of eschbach's hosted Shiftconnector® software in 2021 and 2022. Both black box and grey box tests are performed to verify the cloud-readiness of the application. These tests are based on the guidelines, which represent the most important security risks for web applications.

1 DCSO (Deutsche Cyber-Sicherheitsorganisation GmbH): Founded by Allianz SE, BASF SE, Bayer AG and Volkswagen AG to counter organized cybercrime and state-directed industrial espionage, the DCSO offers various Managed Security Services along the Incident Response Lifecycle and Security Consulting.

2 TÜV Rheinland stands for safety and quality in virtually all areas of business and life. Founded more than 150 years ago, the company is one of the world's leading testing service providers with more than 20,600 employees.

# INCIDENT MANAGEMENT

Our team maintains a comprehensive incident response and forensics program. In the event of an incident that may affect the confidentiality, integrity, or availability of systems or data, we have extensive procedures for detection, communication, mitigation and forensic analysis. Incidents involving the cloud and customer data have the highest priority. We also collaborate with the DCSO for forensic and incident response support.

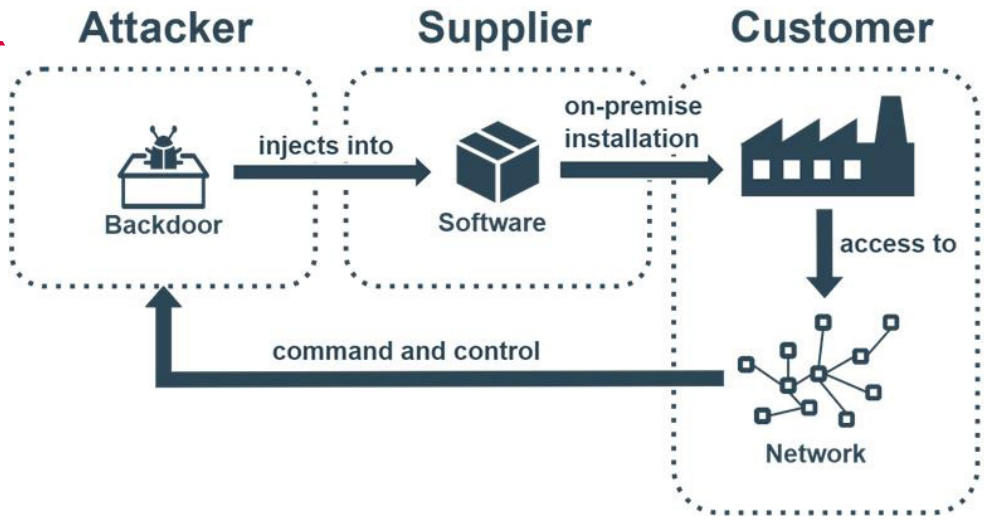
# THREAT LANDSCAPE

To apply the right defending measures and prioritizations, it is important for eschbach to stay informed about its threat landscape. The pharmaceutical industry and its data are a valuable target for threat actors. As a software supplier to these specific industries, we need to be aware of the threats to our customers and ourselves. Because of that, eschbach regularly analyzes its threat landscape and cooperates with the DCSO for that. Based on this intelligence, a security prioritization is made that corresponds to the current threat situation of eschbach and its customers. eschbach is also a member of the DCSO Community, which allows us direct interaction with other experts and access to exclusive content and intelligence.

# SUPPLY CHAIN ATTACKS

Past software supply chain attacks, like the SolarWinds hack, showed the risk of running and updating software inside of your own network and infrastructure. In contrast, the usage of a SaaS-solution provides additional protection against supply chain attacks. By not placing software directly on customers' networks (unlike on-premise installations), customers have an additional layer of security through the browser. Moreover, customers do not have to maintain system security and patching.

But even for SaaS-solutions, corresponding protections from software supply chain attacks are needed. For countermeasures, eschbach developed a comprehensive secure software product lifecycle to protect against supply chain attacks. This software product lifecycle also supports the transformation from DevOps to DevSecOps. You can read more about supply chain attacks, the developed secure product lifecycle and our analyses in our dedicated whitepaper.



eschbach

# To learn more about eschbach and Shiftconnector® reach out to us below.

www.shiftconnector.com
info@eschbach.com

**Europe HQ**: +49 (0) 7761 55959-0
Bad Saeckingen, Germany

**USA & Canada**: +1 (617) 618-5261
Boston, MA

**About eschbach and Shiftconnector®**

eschbach, headquartered in Bad Säckingen, Southern Germany, with a subsidiary in Boston, MA, USA, develops software for plant process management. Shiftconnector® provides a new level of team communication to ensure safety and improve plant effectiveness. The award-winning solution is trusted worldwide by leading manufacturing companies such as Bayer, DuPont, BASF and Roche. For more information visit eschbach.com.

**Disclaimer**