ıllCAM   SCHUıllANN

SCHUMANN Hosting –
Maximum Security and Performance

An overview of the services provided by our private cloud solutions, which offer you flexibility, security and support when utilizing our software.

SCHUMANN Hosting – Maximum Security and Performance

Through diverse connection possibilities, modern backup solutions and constant monitoring, our hosting solutions offer you the flexibility, security and support that you need to achieve your business goals. With flexibly selectable add-ons such as dedicated firewalls, VPN site-to-site connections and geo-redundant backups we can tailor our service exactly to your requirements.

DATA CENTRE SCHUMANN HOSTING

Our infrastructure...

...based on our own hardware in an ISO-certified data centre in Germany that fulfils the highest security standards.

Around-the-clock support

Our bought-in service from the data centre provider guarantees that a team is available around-the-clock to provide support at any time.

Private cloud with own hardware

Our private cloud is hosted on dedicated hardware at a German data centre. This guarantees that no other services run on this hardware, which offers you maximum security and performance.

Flexibility & individual maintenance windows

Thanks to our private cloud we can set dedicated maintenance windows ourselves, without being dependent on other service providers. This enables us to offer you a wide range of service level agreements (SLAs).

High availability and security

The data centre is divided into fire compartments and has contingency plans for emergencies. If a fire compartment fails, the switchover takes place within around 10 minutes, so that long downtimes are avoided. Our infrastructure is designed so that a high availability of all components is guaranteed across both fire compartments.

Certified contact partner

We and all our service partners are ISO 27001-certified, which gives you additional security and trust in our services.

SCHUMANN Hosting –
Maximum Security and Performance

INFRASTRUCTURE, DATA PROTECTION AND MONITORING

Diverse forms of interface

We offer you numerous connection options, including individual firewalls, load balancers and VPN connections in order to fulfil the requirements on compliance and security. All solutions are adaptable and can be tailored to your specific needs.
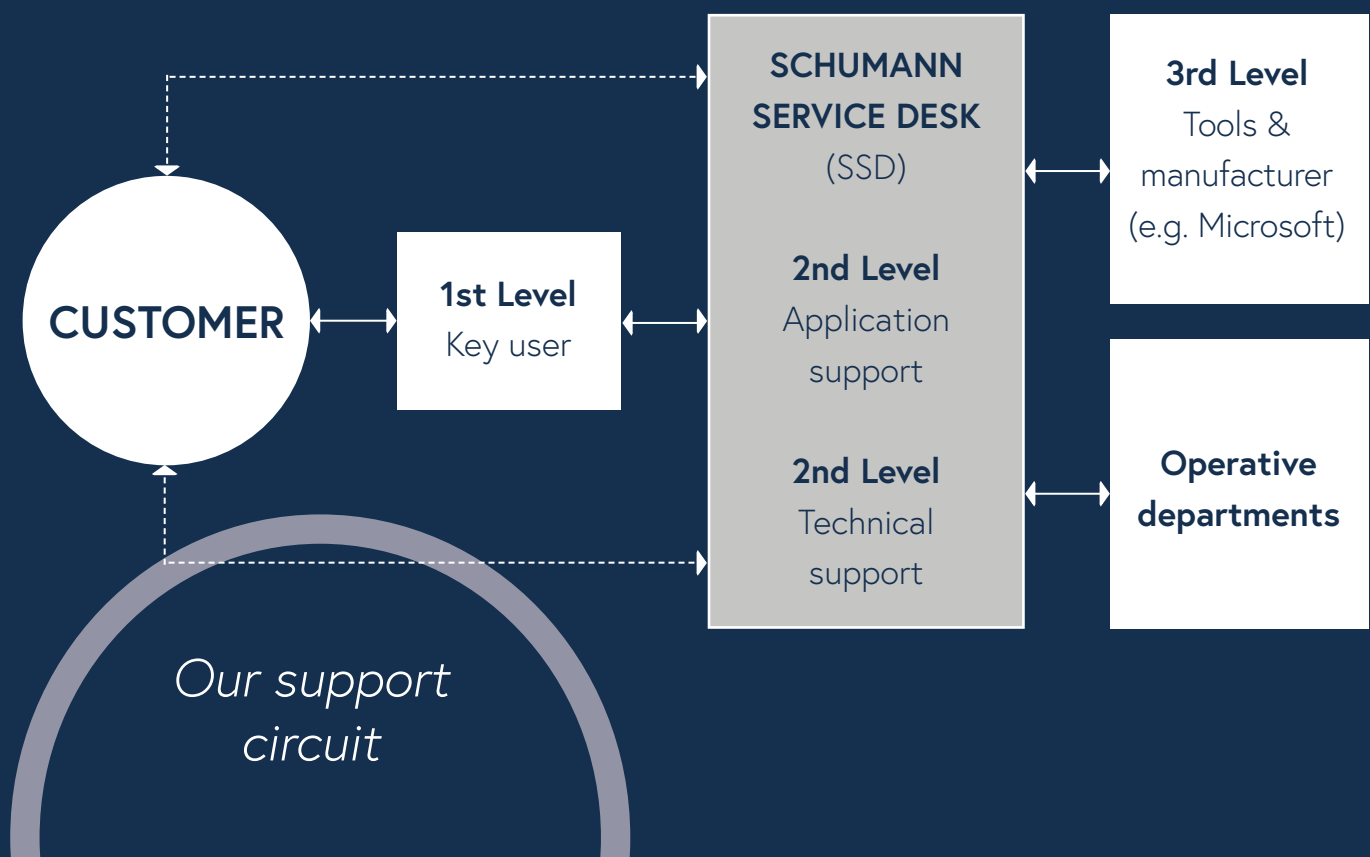
Modern backup solutions

We offer you modern backup solutions that can be geo-redundant if desired. Our backup strategy follows the grandfather-father-child principle with a retention time of 30 days and a frequency of every 24 hours.

Monitoring and reporting

Our monitoring and reporting service uses market-leading software (highly automated, almost unlimitedly scalable, flexibly extendable) in order to offer you a comprehensive overview of your system.

SCHUMANN SERVICE DESK – THE CENTRAL POINT OF CONTACT

With our SCHUMANN Service Desk (SSD) you have a central point of contact for all questions regarding application and cloud support

CUSTOMER

1st Level
Key user

SCHUMANN SERVICE DESK
(SSD)

2nd Level
Application support

2nd Level
Technical support

3rd Level
Tools & manufacturer (e.g. Microsoft)

Operative departments

Our support circuit

SCHUMANN Hosting –
Maximum Security and Performance

ADD-ONS FOR INDIVIDUAL REQUIREMENTS

Add-On	Description
VPN site-to-site ✓ Contact partner: We need a dedicated contact partner on the customer side. ✓ Cooperation obligation: The customer has an obligation to cooperate in analysing errors.	*VPN site-to-site is a technology that enables two or more networks (customers, service providers) to connect with each other securely via the internet. An encrypted tunnel between the locations (sites) is set up so that data can be transferred securely between the networks (via a unified system). The advantages are increased security, data protection and the possibility to share resources and services between the locations.*
Firewall ✓ Own firewall: Per customer or optionally available per stage (productive/ test system).	*A firewall is a security mechanism that monitors and checks the data traffic between an internal network and external sources. It functions as a barrier against unwanted access and threats whilst allowing authorized data traffic.*
Dedicated IP ✓ If desired: Dedicated IP address for all systems belonging to the customer. ✓ IP whitelisting: If required, the customer can perform IP whitelisting. ✓ Per stage: Only if implemented.	*A dedicated IP is a fixed IP address that is exclusively allocated to a particular customer or application. In contrast to a shared IP, which is used by multiple users or services, a dedicated IP enables better control of the data traffic and improve security. It also simplifies the implementation of IP whitelisting. It is often used for web hosting, VPNs and other services for which a unique identification is necessary.*
Load balancer ✓ Dedicated load balancer: Only possible in combination with a dedicated IP address. ✓ Own load balancer: is set up when a dedicated IP is used (not clustered).	*A load balancer is a network device or software that distributes incoming data traffic between multiple servers in order to distribute the load evenly. This ensures that no individual server is overloaded, which improves availability and the performance of applications. Load balancers increase the scalability, enable better use of resources and offer redundancy by automatically redirecting data traffic when a server fails.*

SCHUMANN Hosting –
Maximum Security and Performance

ADD-ONS FOR INDIVIDUAL REQUIREMENTS

Add-On	ℹ Description
Own domain ✓ Combination: Only in combination with a dedicated IP address and dedicated load balancer. ✓ SSL certificate: The customer must provide the SSL certificate.	*Having your own domain in hosting means that the customer uses an individual web address that is connected with SCHUMANN Hosting.*
Geo-redundant backup ✓ Backup solution: Provision of geo-redundant backups for increased data security.	*A geo-redundant backup is a data backup that is stored in multiple geographically separated locations. This ensures that even in the case of a natural disaster, electricity outage or other regional problem, the data is protected. This method increases data security and availability because in an emergency a different copy of the data can be accessed. Geo-redundant backups are especially important for companies that need high availability and data security.*
IP whitelisting ✓ Incoming: Regulation of where the system can be accessed from (this feature can be realized without a dedicated IP address). ✓ Outgoing: Access via the dedicated IP for whitelisting on the customer side (peripheral systems).	*IP whitelisting is a security measure in which only specific, previously determined, IP addresses are allowed to access a network, system or application. All access attempts from other IP addresses will be blocked. This method increases security by hindering access by unauthorized users or devices. IP whitelisting is commonly used in company networks, for cloud services and in security-critical applications.*

Compliance and security: We carry out regular penetration tests and offer solutions for compliance requirements in various industries.