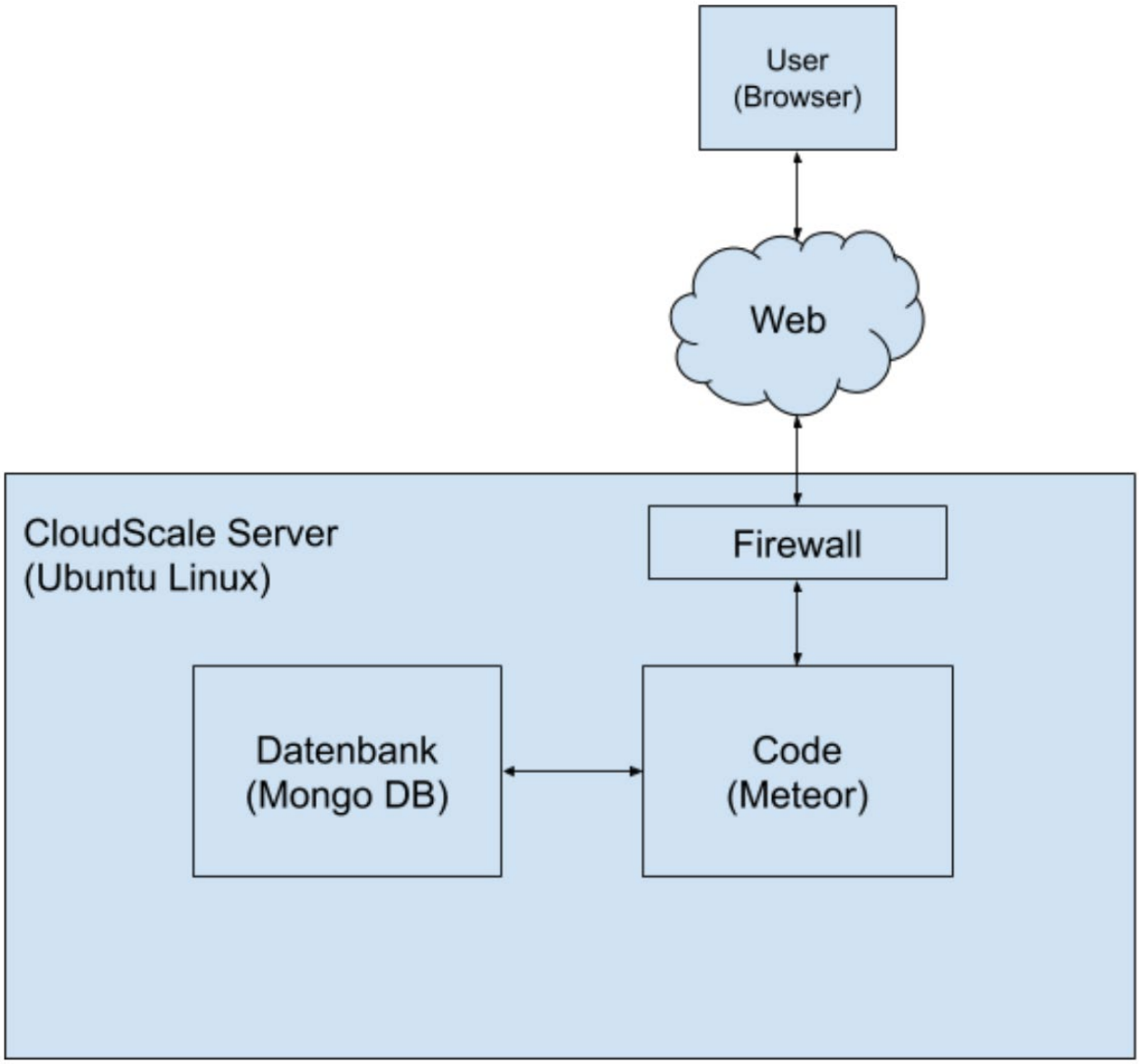
# Summary of the IT architecture of Joineer AG

## IT architecture diagram

The infrastructure of cloudscale.ch AG is hosted by e-shelter Dataschutz AG in Rümlang, Zurich, Switzerland.




The database and code for all Joineer products are located on the Cloudscale server.

The main points of the Cloudscale server infrastructure are described below:

## Physical separation

cloudscale.ch has its own cage, i.e. a separate, closed area within the data centre, in which only our racks are located and to which no third party has access. The contract for this cage was concluded for 5 years (with an option to extend for a further 5 years) in order to be able to guarantee the highest level of physical security in the long term.

## Power supply and redundancy

In this cage, power is routed on two different routes from different sub-distributions, which in turn are connected to different main distributions, to two different power rails per rack. In the event of a power failure, the two main switchboards are supported by separate UPS groups until one of the diesel generators (2N+1 redundancy) takes over the load. The two main switchboards are ring connected to different suppliers (EWZ and EKZ). The redundancy is tested by the data centre operator at regular intervals (so-called autarkic tests). All our systems are connected to both circuits, so that we can cope with the failure of one power supply unit - or an entire circuit - without noticeable impact on operations.

## Air conditioning

The data centre area is free of water pipes and is surrounded by an air conditioning coil (air cooling units with recirculated air: 2N redundancy). The water is routed in a ring so that in the event of a defect, individual sections can be interrupted and repaired without endangering the supply line to the other recirculating air-cooling units. The building is also equipped with a free-cooling system on the roof. This means, for example, that in winter, when temperatures are cold, the areas are cooled with significantly less energy consumption. In addition, E-Shelter is the first data centre in Switzerland to comply with the ISO50001 standard.

## Internet connection

The internet connection of cloudscale.ch is provided via two different routes (so-called route redundancy) to the two operator meeting rooms in the building. These in turn are accessible via two separate entrances to the building (on opposite sides of the building). cloudscale.ch deliberately uses two different operators with different data protection. cloudscale.ch deliberately uses two different operators with different hardware suppliers (Init7 with Brocade/Extreme hardware, Liberty Global with Cisco hardware) and is also present on the SwissIX Internet Exchange. cloudscale.ch operates the standalone system 59414. https://bgp.he.net/AS59414#_asinfo

*What technical measures are implemented to protect the host (host firewall, regular integrity checks, host-based intrusion detection systems)?*

## Network

Physical separation of management and customer traffic (separate and redundant network equipment, multi-vendor strategy).
Physical separation of Internet access traffic and storage access traffic (separate and redundant network connections).
Logical separation of public and private client traffic (private and client-specific VXLAN).

IPtables and ebtables on each hosting computer:
- Each virtual server (VM) has a fixed IP/MAC address pair and can only communicate with it.
- Prevention of "man-in-the-middle" attacks in the public network
- Prevention of sniffing in the public network
- Complete logical separation in the private network thanks to private and customer-specific VXLAN.

## Controller

Physical separation of the host control device, the hosting computer and the host storage device
Logical separation of control services in LXC containers.
Management access to the physical machine is only possible from the dedicated management network (no internet exposure).

## Data processing

Kernel virtualisation with QEMU/KVM (full virtualisation, separate QEMU process per VM).
Memory is permanently allocated per client, even when the VM is turned off (no memory bloat or merging of identical pages in the kernel).
Many "0-day" security failures cannot be exploited on Ubuntu thanks to AppArmor.
Consistent use of ECC memory (e.g. Rowhammer attack is almost impossible).
Management access to the physical machine is only possible from the dedicated management network (no internet exposure).

## Storage

Separate RBD volume per client and per volume in the VM (replication factor 3, spread over 3 different racks).
Management access to the physical machine is only possible from the dedicated management network (no internet exposure).

## Control panel

Only salting and hashing are used for storing login passwords.
Optional two-factor authentication (TOTP)
Display of SSH host key fingerprints per VM
Consistent use of CSRF prevention
Session management with overview

*How does Cloudscale ensure a secure basic configuration of the host (e.g. use of hardened operating systems, disabling unnecessary services, etc.)?*

To ensure a uniform configuration (firewall rules, disabling unnecessary services), we use Ansible as a configuration management tool. We use Ubuntu LTS (Long Term Support) as our operating system, which is particularly suitable for server use. Each LTS version is supported for at least 5 years after its release (security updates).

## Additional information

If desired, we can also send you two BDO reports (ISAE 3000 and FINMA audit report), which will cover many security issues. In consultation with Joineer, the client is invited to audit (or have audited) the architecture of cloudscale.ch. CloudScale charges CHF 225 per hour (excluding VAT) for this and the audit must take place at Cloudscale's offices.