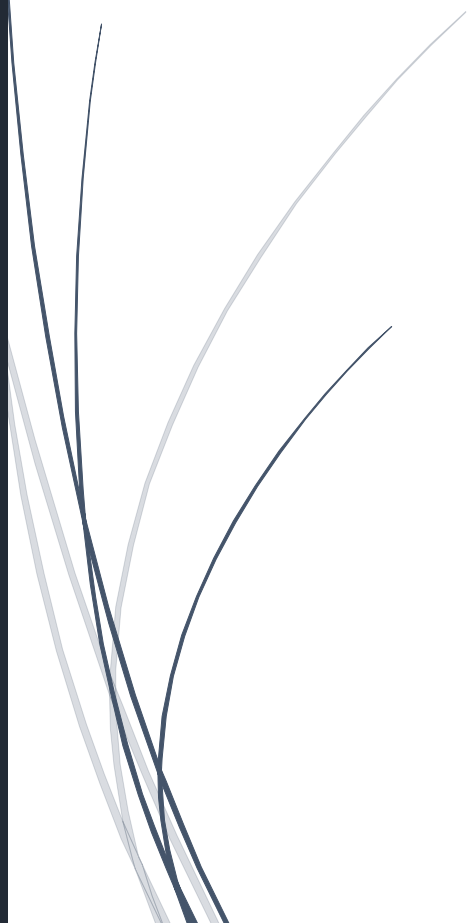


Holistic IT infrastructure





The ideal and secure IT network infrastructure

The requirements for the network infrastructure of a company, state organisations, municipalities and cities are constantly increasing. A multitude of software and hardware components must function together, be managed and maintained. With the complexity of the IT infrastructure, the administration, acquisition and maintenance costs increase. But the vulnerability and the risk of security gaps and failures are also increasing. In addition, the dependence on many different suppliers and specialised personnel is growing massively.

Employees today are mobile. They work in the office, on the road, from home, with local or remotely deployed applications or on cloud-based solutions. This increases the risks exponentially. The user's end device, home network or hotspots from which they work, where possible malicious applications could be on third-party devices or in that network, make "secure" work impossible. The whole thing is made even more difficult by communication via the insecure medium of the internet.

Non-compliance with regulations, penalties for cyber attacks and recurring hardware and software costs, rising energy and CO2 emission costs are also a burden on companies.

Maintaining security remains fragile

Even companies that invest a lot of money in hardware, software and personnel struggle with the fragility of their network infrastructure.

Ensuring business continuity, maintaining operational capability is associated with the greatest effort.



Holistic IT infrastructure

A holistically designed IT infrastructure encompasses all these requirements, minimises risks and ensures an uninterrupted platform for business continuity.

It allows flexibility and scalability for future growth or change, reduces complexity and minimises hardware and software requirements. Availability, durability and protection against cyber-attacks and the risk of "hardware failures" are greatly minimised. At the same time, energy consumption and thus CO2 emissions are greatly reduced.

A holistic IT infrastructure consists of the three components that form the pillars as a tripod. Even if each of the components can be operated independently and represents a high-quality and secure solution in its area of application, they represent the holistic, highly secure IT infrastructure as a unit in interaction with each other.

The tripod for IT infrastructure builds a protective shield against unwanted influences from outside and inside and ensures availability and scalability of the infrastructure.

- sayFUSE HCI-Plattform

- sayFUSE Backup and Restore Platform

- sayTRUST VPSC

- provides a **scalable, fail-safe high-security infrastructure** and protects your company or organisation against cyber-attacks and disasters.
- **provides an ideal solution for companies or organisations of any size.** Forms an ideal platform for data centres, banks, cities and municipalities that value quality, security, above-average performance and sustainability.
- provides an **infrastructure for one or more locations, clients or departments.**
- offers an advanced **high-speed platform for Big Data analytics.** For very large and diverse data sets, structured, semi-structured and unstructured data from different sources and in different sizes (from terabyte to zettabyte).

The sayFUSE HCI platform forms the basis for sustainable business continuity that can be scaled as required. It reduces the complexity of the entire IT infrastructure and minimises hardware and software requirements. Installation, migration and operating costs are sustainably reduced. Hardware replacement cycles are significantly extended and electricity costs and CO2 emissions are significantly reduced.



The integrated hypervisor ensures the creation of a coherent storage, computing and networking across the individual nodes and provides all infrastructure components as a multi-tenant service. The sites/clients can receive their infrastructure as a service and do not need to purchase additional servers and storage in the future. They can use all the services provided in their IaaS via their isolated infrastructure.

- | | | | |
|----------------|---------------------|----------------------------|------------------------|
| ✓ Firewall | ✓ Floating-IP | ✓ NFS-, iSCSI-, S3-Storage | ✓ Trackless Zero Trust |
| ✓ Router | ✓ Virtual Server | ✓ Kubernetes | Communication |
| ✓ Loadbalancer | ✓ Virtual User-PC | ✓ Single Sign-on | ✓ Personal Key |
| ✓ VPN | ✓ Multilevel Backup | ✓ Application Publication | Identification |

The individual IaaS of the locations or clients are isolated from each other and from the insecure internet as well as from the in-house network and are not visible. The access of users to the individual applications, services, networks or their own virtual PC takes place via the sayTRUST VPSC technology, after checking the identity of a user via the multi-level Defence in Depth security procedure.

sayFUSE Backup (Fast Universal Storage Backup Engine)

The sayFUSE backup solution offers a unique **high-speed backup with up to 12 TB/hour for live backup and with up to 18 TB/hour for migration backup**. The technology eliminates all typical backup vulnerabilities of tape and storage-based technologies. It also **bundles all six essential backup components**. Backup Server, Backup Storage, Backup Library, Backup Drives, Media Break and Offload in one unit. It provides high backup quality and ensures the recoverability of data and systems. Within the backup appliance, the data is migrated from the backup storage to the integrated backup library system and swapped out.

sayTRUST VPSC (Virtual Private Secure Communication)

The sayTRUST VPSC as a Zero Trust Client Access solution, enables secure communication independent of location, device and topology and ensures a highly secure working environment. sayTRUST VPSC offers the highest level of communication security by **detecting and eliminating vulnerabilities between the user and the network to be protected**. Users can work securely within their own network as well as from external locations, home offices or mobile hotspots via the 8-stage "Defence in Depth" Zero Trust technology.

sayTRUST VPSC enables tunnelled communication for **local, remote and mobile applications**. Server-side generated user certificates via the own "Certificate Authority" **control the allowing, blocking and isolating** of applications and resources. Encrypted communication begins after the user's identity has been verified and is **encrypted within the application level from the client's RAM. Memory (RAM) of the client PCs**, instead of via network-network coupling.

The products sayFUSE HCI, sayFUSE Backup and sayTRUST VPSC can also be operated independently of each other and each represents a highly secure and unique solution in its respective field of application. In combination, they reinforce each other and form a holistic infrastructure solution for the requirements of today and the future.