secunet

For digital sovereignty and transparency in the cloud

Cloud infrastructure solutions

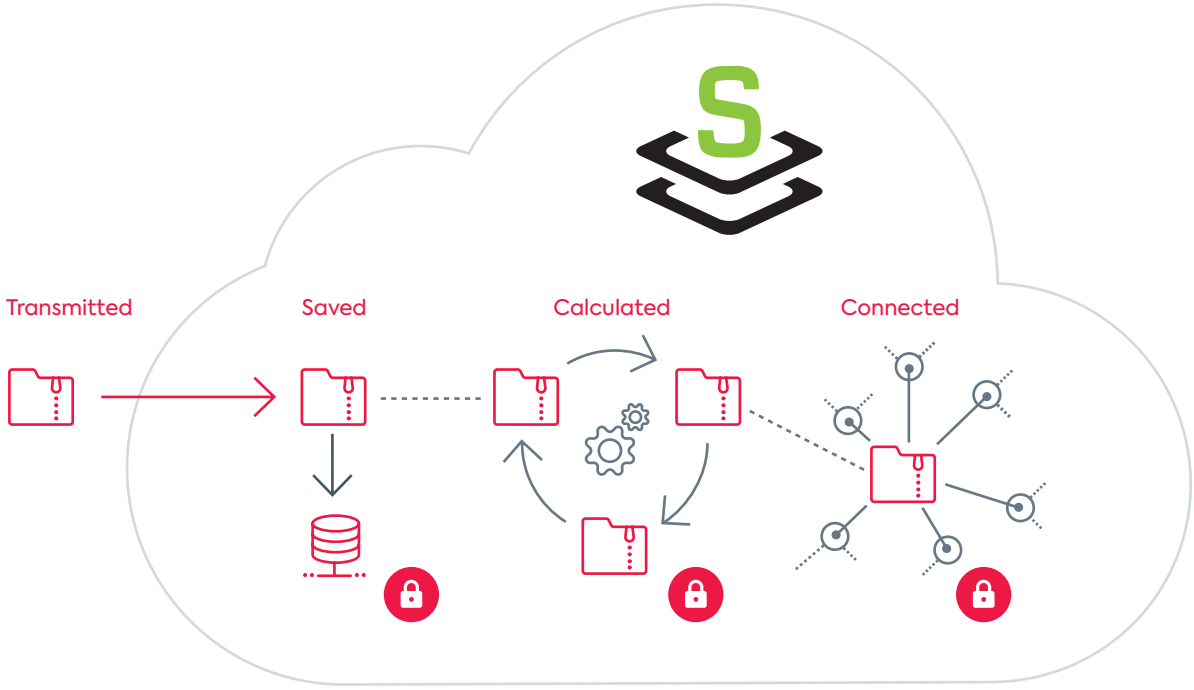
Digital sovereignty and trustworthiness in the cloud

Shared use of infrastructure not only saves resources but also enables companies to push ahead with digitalisation with limited technical expertise and little effort. Security, trustworthiness and transparency are however essential to prevent this from leading to digital dependency. SecuStack® enables companies to retain full control over their processed and stored data. SecuStack® is a cloud operating system which enables simple and secure provision of resources for the operation of cloud applications by acting as an "Infrastructure as a Service" (IaaS).

It is fully compatible with OpenStack, being an extension of it. Transparently integrated cryptographic mechanisms now consistently safeguard the transfer, storage and processing of data as well as the networking of resources in an OpenStack environment. SecuStack® thus enables access to cloud computing for various sectors, which have been as yet unable or unwilling to use cloud computing due to strict security regulations or lack of trust.

Benefits

- Use of open-source technology
- Avoidance of vendor lock-in effects
- Optionally on-premises or hosted
- Maximum transparency of the infrastructure
- Digital infrastructures made in Germany



SecuStack® – the secure cloud operating system

A comparison of IaaS, PaaS & SaaS usage

Cloud usage by German companies is steadily increasing, and the Covid-19 pandemic has brought another positive boost. Two-thirds now use private cloud models, half of which use public clouds (Bitkom Cloud Monitor, 2021).

Among German companies that rely on private clouds, SaaS is the service most in demand, at 46 %. However, IaaS (34 %) and PaaS (29 %) are also being used more frequently, with double-digit annual growth rates in some cases (Gartner, April 2021).

"as a Service" models vs. "lock-in" effect
In cloud business models, verticalisation and monopolisation in the form of provision "as a Service" can be observed. A high degree of complexity and increasing dependence on the specialised tools for using the services of large platforms leads to a "lock-in effect", which makes it difficult to switch to another provider and prevents digital sovereignty.

IaaS: Infrastructure as a Service
The fundamental level of cloud computing is IaaS, because this is where hardware resources are provided in virtualised form.

Whether storage space, processors or network – all computing instances can be added and removed in any quantity. This is why it is sometimes referred to as a virtual data-centre.

IaaS is probably where the cost advantages of cloud computing come into their own most clearly: Hardware is particularly expensive to purchase, quickly becomes outdated and should also be set up under particularly secure conditions (keyword: data-processing centre vs. company basement). If the provision of IT resources is virtualised and demand-oriented, users typically make enormous savings.

PaaS: Platform as a Service
PaaS is the link between IaaS and SaaS and enables the interaction of the other levels.

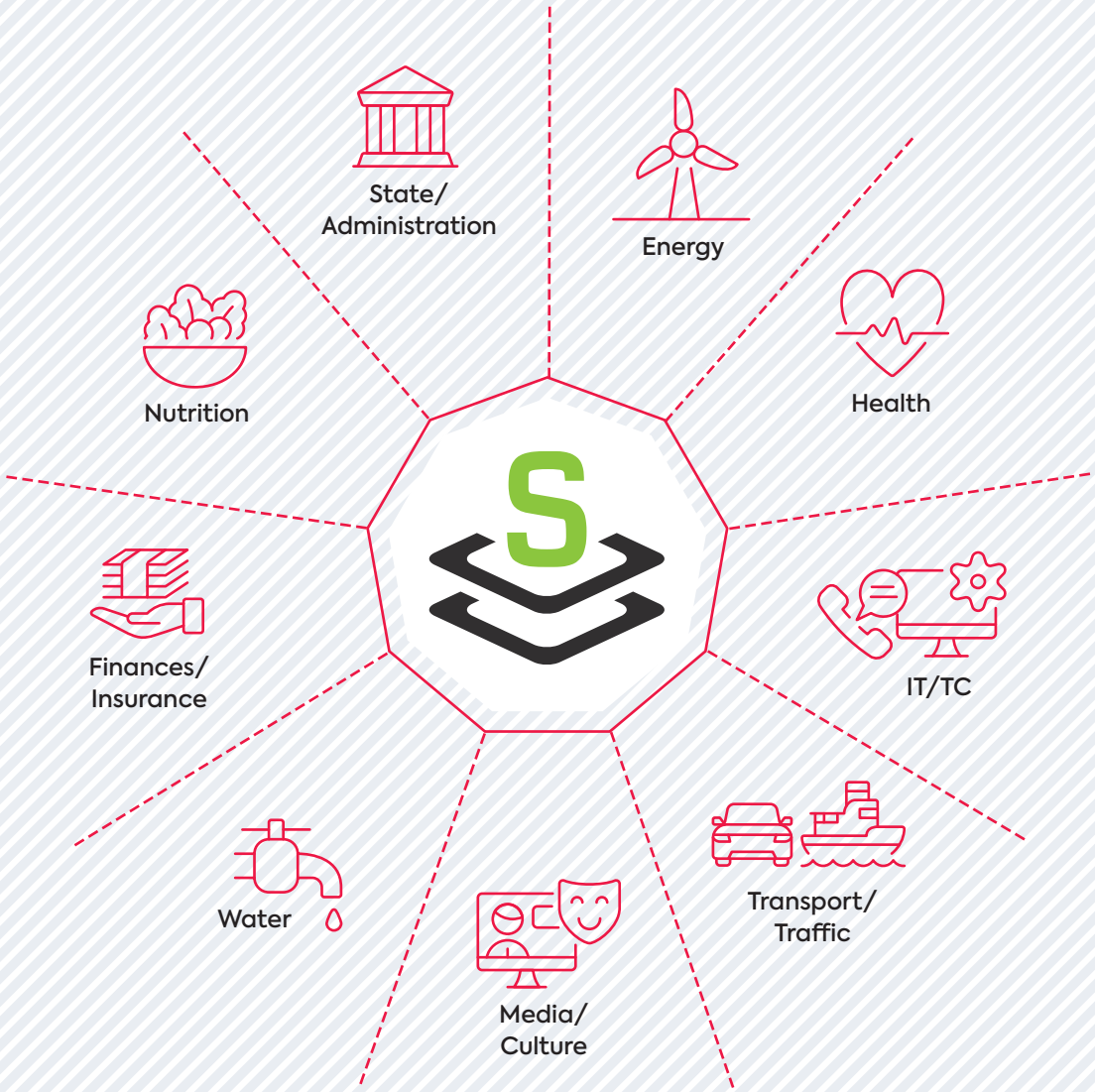
This is because the development and runtime environments for software are provided at the platform level, building on IaaS resources such as operating systems. The other two levels – IaaS and SaaS – are usually addressed through APIs. As a result, software developers are particularly interested in PaaS.

SaaS: Software as a Service
With SaaS, programmes are provided on demand – usually directly to the end user.

Usage usually takes place via the Internet or a web browser. Through SaaS, users can usually save on licence fees and also do not have to pay for installation and administration.

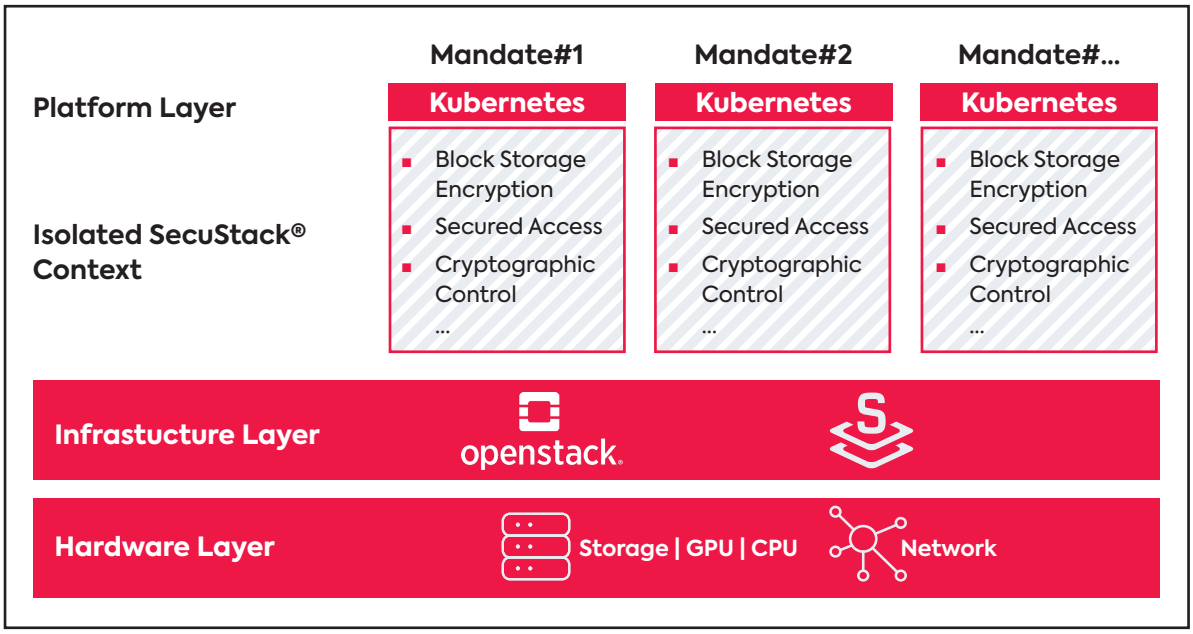
Areas of application for SecuStack®

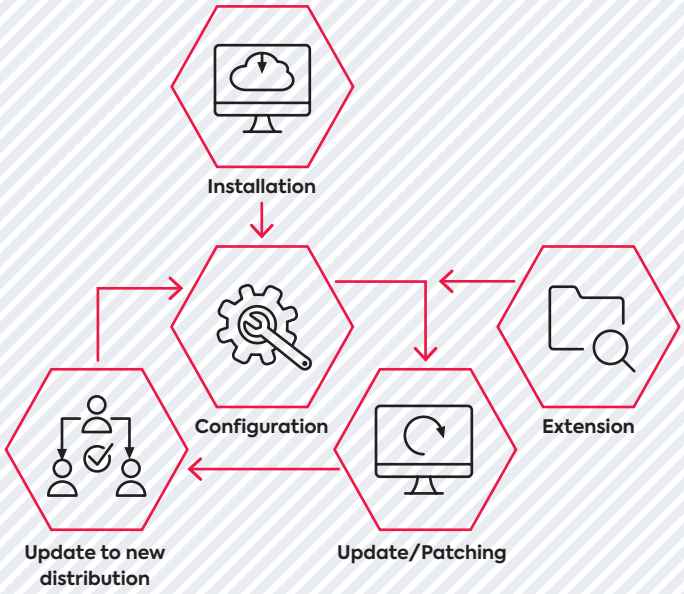
SecuStack® enables security-compliant and trustworthy cloud computing for a wide range of industries



Secure application processing in the cloud

Container orchestration
Deploying, scaling and operating applications has never been more secure. By adding isolated cloud contexts to the SecuStack® security-hardened infrastructure base, individual or multiple applications, or even the entire computing cluster can be run in isolated container environments managed by Kubernetes. Each cloud context also offers the advanced SecuStack® security aspects.





Reduction of costs and complexity

SecuStack® Lifecycle Management
By using the Lifecycle Management Service, SecuStack® enables companies to reduce the costs and complexity of their own IT operations.

The SecuStack® Lifecycle Management Service includes installation as well as simple integration and management of extensions and updates in terms of the infrastructure base and current security enhancements. In this way, the digital infrastructure can always be kept up to date.

SecuStack® enables security-compliant and trustworthy cloud computing for a wide range of industries

The decision in favour of a cloud model or a cloud service is an individual and needs-oriented decision that must be made depending on the industry and regulations.

In all cloud models, scalable computing resources are aggregated, bundled and shared over a network. Classic cloud computing.

They allow workloads to run on the respective system and comprise a specific combination of technologies, locations and proprietary rights.

Public cloud

- Offered by third parties
- Available to everyone via the public Internet
- Quickly and conveniently scalable

Private cloud

- Offered to a selection of users via the Internet
- Provides better security checks
- Requires traditional staff resources and maintenance in the data centre

Hybrid cloud

- Combination of public and private cloud
- Shared security responsibility
- Helps maintain tighter controls over sensitive data and processes

SecuStack® architecture

Cloud environment with SecuStack®

SecuStack® is an OpenStack-based trusted, secure and auditable cloud operating system.

User software	**Your applications** (such as KI/ML, SAP, Wordpress, ...)
Platform	**Your platforms** (such as Kubernetes, OpenShift, ...)
Operation & Monitoring	**SecuStack® O&M**
IaaS/VMs	**SecuStack® CORE**
Operating system	**SecuStack® INFRA**
Storage | GPU | CPU **Network**	**Hardware infrastructure** (hosted by you on-prem and/or in a trustworthy manner)

SecuStack® – Difference to OpenStack

Feature	OpenStack	SecuStack®
Block storage encryption	✓	✓
Image encryption	✗	✓
Automatic key management	✓	✓
Bring your own Key (BYOK)	✗	✓
Hold your own Key (HYOK)	✗	✓
Flexible hypervisor-host separation	✗	✓
Client network encryption	✗	✓
VPN as a Service for client networks	✗	✓
Full PKI integration	✗	✓
Infrastructure protection	Manual	✓

SecuStack® at a glance

Holistic security concept

1. **Secure cloud infrastructure**
   - Consistent encryption of the data
   - End-to-end security (VPNaaS and key management concept)
   - Cryptographic separation of clients
2. **Secure Lifecycle Management**
   - Installation & configuration
   - Updating & upgrading
   - Monitoring & alerting
3. **Secure container orchestration**
   - Secure processing of applications n the cloud
   - Support for the control and automation of isolated computing tasks – especially in large dynamic environments
4. **Secure operating concept**
   - Holistic, standardised operating concept according to security requirements
   - Total stack protection: full control of physical and virtual machines
5. **Turnkey Solution**
   - Hardware & software from one provider
   - Turnkey configuration
   - Adapted to individual requirements

Product portfolio – SecuStack®

SecuStack® CORE

SecuStack® tackles strong, multi-layer client separation, which is primarily based on cryptographic mechanisms.

Secure access
Secure, encrypted access to the cloud infrastructure.

Client network protection
Isolated, encrypted client networks.

Secure images
Image encryption and additional security through digital signature.

Infrastructure hardening
Mechanisms and advisory services to secure the underlying infrastructure.

Block storage encryption
Complete encryption of stored user data and access restriction.

Cryptographic control
Full control over the cryptographic keys used.

SecuStack® INFRA

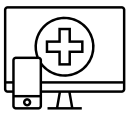
SecuStack® INFRA is based on SecuStack® CORE and offers automated provisioning for SecuStack®. It defines a system architecture with focus on high availability and scalability. All OpenStack/ SecuStack® components are redundant, so even if individual server systems fail, the SecuStack® cluster remains available.

SecuStack® O&M

SecuStack® Operations&Management (O&M) is based on SecuStack® INFRA and offers complete life-cycle management for managing an OpenStack environment. This keeps the SecuStack® infrastructure "as a service" up to date and operational.

If a problem occurs within the cluster, an operator is automatically informed of the problem on a 24/7 basis, thanks to a monitoring system. In case of critical problems, the operator responds in less than an hour after the problem is detected and starts to identify the cause of the problem.

Use Cases



Healthcare

Health and patient data are increasingly processed in hyperconvergent ICT infrastructures. Local and central systems merge into each other, cross-organisational process routines establish themselves. Today, the virtualised and centralised IT services are often still operated „on premise“ due to compliance specifications.

Cloud migration is subject to extensive regulatory requirements.

SecuStack® enables operators and providers of software solutions to transfer their current solutions to a cloud operating model that meets the special security requirements of German legislation. A trusted cloud infrastructure is being created as a security-hardened open-source cloud that connects all areas of medical care, e.g., patient data systems, medical technology, evaluation analytics and medical robotics.

Police and civil protection

Police and security authorities depend on fast and legally certain communication, not only in the event of disasters or confusing situations. The daily work is carried out by the authorities via digital radio communication. Messenger apps are also becoming increasingly established, although not in the sense of WhatsApp and similar apps.

Typically, the infrastructure of the security authorities is operated by the country's own IT providers in order to ensure full control over the data. Messenger apps such as stashcat are administered centrally and the corresponding apps are installed on police-owned or private (BYOD) mobile phones. SecuStack® offers a reliable platform on which these services can run and be operated in a legally secure manner.

Utilities: Edge cloud

The energy transition is probably the most important project in our society today. Besides environmentally friendly energy generation, the greatest challenge at present is intelligent distribution and storage. At the same time, energy demand is increasing due to new data centres being built to host cloud services.

With a SecuStack® Edge Cloud, energy providers rely on a model that uses surplus energy directly where it is generated. In small decentralised data centres, energy is converted into computing power without feeding it into the grid. This increases the efficiency of plants and reduces costs for providers and consumers.

Authorities & administration

Administrative modernisation cannot be realised without modern cloud technology. However, established hyperscalers do not seem to offer a sustainable solution here, as they are unsuitable for government and sovereign IT services from a political (digital sovereignty), business (vendor lock-in effects) and data protection perspective.

As a security-hardened solution based on open source, SecuStack® offers full control and sovereignty on the technology used and the required operating mode – whether "on premise" for a dedicated private cloud or in established operator models with multiple customers under strict cryptographic client separation. Specialist procedures, web portals, online services and collaboration tools receive a fully auditable and innovative foundation with SecuStack®.

VS Cloud for armed forces and authorities

The ultimate in data security is the handling of classified documents (RESTRICTED/VS). They are classified by sovereign authorities and comprise sensitive administrative documents, military mission data or even state secrets. The security measures taken to protect them seem excessive and inefficient in a private sector environment. At the same time, they form the everyday basis of state activity.

The SecuStack® infrastructure layer, designed in collaboration with IBM, RedHat and secunet, is based on an extensively hardened open-source approach.

The design principles and security technologies used are the same as those used in the VS-approved SINA products, which were developed in cooperation with the German Federal Office for Information Security (BSI). SecuStack® is expected to establish itself as a cloud solution for VS-classified information. An evaluation process for a VS-NfD (restricted) project in a federal authority is currently taking place in cooperation with the BSI. Additional hardening measures are being implemented in parallel to make cloud solutions possible beyond the scope of VS-NfD and to have a concrete perspective of use in the upcoming „German Mission Network" of the German Federal Armed Forces.

Private cloud with client separation

If the data and applications of several organisations are processed in a central cloud infrastructure, a strict separation of services and clients must be ensured. In existing approaches, the separation takes place on the physical level. Separate racks with independent and disjoint components such as virtualisation solution, network and hardware must be procured and operated for each client. Especially the licensing of the market-leading proprietary software solutions (e.g., VMware, Microsoft, Citrix, Oracle ...) generates considerable costs.

The SecuStack® technology enables client separation to be carried out at a higher level of abstraction. Strict cryptographic separation and flexible key management allow different clients to use the same components without compromising data protection and security. This significantly better utilisation of existing hardware resources and the lower licensing costs provide a considerable cost advantage.

secunet – Protecting Digital Infrastructures

secunet is Germany's leading cybersecurity company. In an increasingly connected world, the Company's combination of products and consulting assures resilient digital infrastructures and the utmost protection for data, applications and digital identities. secunet specialises in areas with unique security requirements – such as cloud, IIoT, eGovernment and eHealth. With security solutions from secunet, companies can maintain the highest security standards in digitisation projects and advance their digital transformation.

Over 700 experts strengthen the digital sovereignty of governments, businesses and society. secunet's customers include federal ministries, more than 20 DAX-listed corporations as well as other national and international organisations. The company was established in 1997, is listed in the Prime Standard segment of the Frankfurt Stock Exchange and generated revenues of 285.6 million euros in 2020 (preliminary business results as at January 22nd, 2021).

secunet is an IT security partner to the Federal Republic of Germany and a partner of the German Alliance for Cyber Security.

secunet Security Networks AG
Kurfürstenstraße 58 · 45138 Essen · Germany
T +49 201 5454-0 · F +49 201 5454-1000
info@secunet.com · secunet.com

secustack

SecuStack® was founded by IT security specialist secunet Security Networks AG and IT infrastructure provider Cloud&Heat Technologies GmbH. Through this collaboration, the two partners combine their many years of expertise in the field of security solutions and the operation of OpenStack-based cloud infrastructures.

gaia-x

GAIA-X – Data Sovereignty for Europe Day one member.

Federal Ministry for Economic Affairs and Energy

IPCEI – Next Generation Cloud Infrastructures and Services