

Press Release

SecuStack uses SCONE and Intel® Software Guard Extensions for novel secure cloud applications

[Essen, Germany, 17 September 2020] SecuStack, the security-hardened cloud operating system made in Germany, will soon support Intel® Software Guard Extensions (SGX) enclaves, based on Scontain's SCONE platform. This will enable cloud applications specific to the fields of machine learning (ML) and multi-party computing to exchange data securely. For instance, two hospitals can use ML models for exchanging and processing patient data, while the data remains protected from access by the cloud provider. Intel SGX also allows data exchanges to occur that do not require trust from the cloud service provider.

secustack GmbH, provider of the SecuStack platform, is a joint venture between secunet Security Networks AG and Cloud&Heat Technologies GmbH. SecuStack addresses companies and public authorities with security-critical applications.

SecuStack is a cloud operating system enabling the simple and secure provision of resources for the operation of cloud applications using "Infrastructure as a Service" (IaaS). As an extension of OpenStack, it is fully compatible with it. Transparently integrated cryptographic mechanisms provide the ability to make the transfer, storage and processing of data as well as the networking of resources in an OpenStack environment consistently secure. SecuStack thus enables various industries to enter cloud computing, which have not yet been able or have not wanted to due to strict security regulations or a lack of trust.

One example is the healthcare sector. As healthcare systems have become more digital, patient health data have previously often been unavailable to hospitals due to privacy and security laws. Now

Press Release

authorised institutions can use, aggregate and analyse anonymised raw data to gain important medical insights.

On CPUs equipped with Intel SGX, critical infrastructure services like Identity Management, Key Management as well as VPN services can be executed inside of trusted hardware-protected enclaves. Intel SGX provides another layer of protection for the integrity and confidentiality of program code and data outside the CPU, thereby greatly increasing the hurdle for attackers. This will provide additional protection of the infrastructure layer that had previously been missing. With the help of Scontain's SCONE platform, services can be easily integrated and executed in Intel SGX enclaves. Functions such as transparent runtime encryption, secrets management and authorization can be integrated very securely. The combination of both Intel SGX enclaves and an open-source-based hardened and cryptographically-secured infrastructure layer provides the most advanced protection today. It provides security and sovereignty of applications and data as well as the integrity of the infrastructure layer.

In addition to infrastructure protection, SecuStack also supports Confidential Cloud Native Applications. Application services can run inside Intel SGX enclaves within a Kubernetes cluster, for instance. One focus is to enable confidential machine learning to permit clients to learn their TensorFlow and PyTorch model in a secure context - protecting training data, code and the models that even the cloud provider cannot gain access to. This will enable novel applications like the following. Hospitals which use a secure cloud infrastructure with SecuStack can perform local, confidential machine learning using the SCONE platform. The local models can be combined with models of other hospitals with the help of confidential federated machine learning: this ensures that models can securely be learned between hospitals, i.e., patient data never leaves the premise and the privacy of the patients is protected at all times.

For more information on SecuStack, please visit www.secustack.com.

secunet



Press Release

Press contact

Patrick Franitza
Spokesman

secunet Security Networks AG
Kurfürstenstraße 58
45138 Essen/Germany
Phone +49 201 54 54-1234
Fax +49 201 54 54-1235
E-mail: presse@secunet.com
<http://www.secunet.com>

About secunet

secunet is one of the leading German providers of high-quality IT security. Over 600 experts work in the areas of cryptography, e-government, business security and automotive security, and develop innovative products in these fields in addition to highly secure and reliable solutions. Many DAX companies as well as numerous authorities and organisations are among secunet's national and international customers, which total over 500. secunet is IT security partner of the Federal Republic of Germany and partner in the Alliance for Cyber Security.

secunet was founded in 1997 and achieved revenues of 226.9 million euros in 2019. secunet Security Networks AG is listed on the Prime Standard of the German Stock Exchange.

Further information can be found at www.secunet.com.

