Case Study

Cloud Service Providers
Security-Enabled Cloud

Making the Cloud More Secure

A security-hardened cloud operating system, SecuStack supports Intel® Software Guard Extensions enclaves—bringing security-enabled cloud computing to a new class of users, including government and highly regulated industries.

At a Glance

- A robust and verifiable foundation for infrastructure as a service (IaaS) on an open source solution
- Transparency and total control over the software stack and data
- Hardened OpenStack plus Intel® Software Guard Extensions (Intel® SGX) provides end-to-end protection for confidential workloads
- Now you don't have to "trust" the cloud service provider (CSP)—SecuStack opens up cloud computing for security-focused organizations

What if you could use public cloud services yet remain confident that your data—in motion, at rest, and in use—is completely under your control? That is exactly what SecuStack aims to achieve, unlocking the benefits of cloud computing for governmental institutions and highly regulated industries. The brainchild of secunet Security Networks AG (Germany's leading cyber security company) and Cloud&Heat Technologies GmbH (a provider of energy-efficient, scalable and secure data center solutions), SecuStack brings cloud computing to various industries who previously have not been able to adopt cloud computing due to strict security regulations or a lack of trust.

Challenge

Cloud computing offers appealing cost, operational efficiency and scalability benefits—but some industries, along with governmental institutions, have not broadly adopted cloud computing due to security concerns. Without transparency into the software stack, and total control over their data, cloud computing remains out of reach for these organizations.

Solution

By providing a security-hardened cloud operating system (OS), SecuStack enables on-premises or trustworthy hosted operation of a modern cloud solution through infrastructure as a service (IaaS). It provides transparency for the functionality of the software stack, unlike commercial software or many cloud service providers (CSPs). SecuStack includes transparently integrated cryptographic mechanisms that help protect data transfer and storage, plus integration of Intel® Software Guard Extensions (Intel® SGX) enclaves that help protect data during processing in an OpenStack environment.

Results

Organizations with strict security compliance needs can now take advantage of all the benefits of cloud computing. These include avoidance of infrastructure expense, reduced maintenance costs, increased operational efficiency, scalability and access to the latest innovations in Intel® technology for high performance.

A Need for Transparency and Control in the Cloud

The cloud is an as-a-service business. Typically, CSPs give their customers services and application programming interfaces (APIs), but not software and source code. Consumers of cloud services, therefore, must trust the CSP that runs the servers, controls the software stack and protects customers' data. Cloud computing may provide a range of benefits, such as efficiency and cost reduction, scalability and disaster recovery capabilities.[1] However, complete transparency and control over the security of data at rest, in motion, and in use is a concern for many government

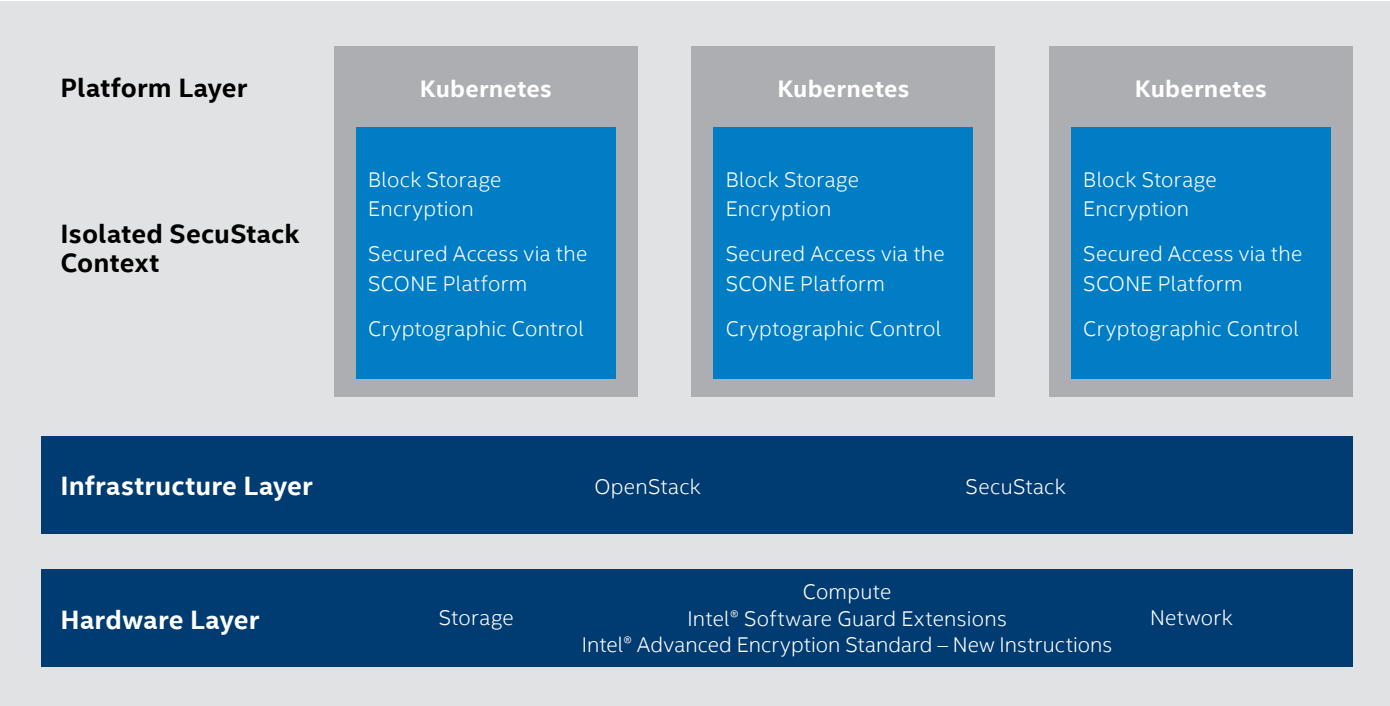

Figure 1. By taking advantage of Intel® Software Guard Extensions (Intel® SGX), the SecuStack operating system enables confidential computing in the cloud.

institutions and agencies, and highly regulated private industries such as utilities and healthcare providers. These concerns have historically proved a barrier to cloud service adoption for these organizations. Without transparency and control over their data, these organizations simply cannot take advantage of external cloud services. Enhanced data protection will also allow enterprises using cloud resources to compute on their data in a confidential manner.

Digital Sovereignty in the Cloud

SecuStack takes advantage of Intel® processors equipped with Intel SGX, which enables critical infrastructure services like identity management, key management and virtual private network (VPN) services to be executed inside of isolated application enclaves. The enclaves have hardware-assisted confidentiality and integrity-added protections to help prevent access from processes at higher privilege levels. Through attestation services, a relying party can receive some verification on the identity of an application enclave before launch. With these capabilities, applications are prepared for more security. With the help of Scontain's SCONE platform, services can be easily integrated and executed inside Intel SGX enclaves. Functions such as transparent runtime encryption, secrets management and authorization can be integrated conveniently. The combination of Intel SGX enclaves and an open source-based hardened and cryptographically secured infrastructure layer provides advanced protection because it helps boost 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 of Intel SGX enclaves running in a Kubernetes cluster, for instance (see Figure 1). SecuStack also uses Intel® Advanced Encryption Standard – New Instructions (Intel® AES-NI) to accelerate SecuStack's encryption processes.

"Many platform providers can offer cloud technologies or artificial intelligence (AI) features. Intel is the only company that can provide cloud and AI technologies in a holistic, secure way."

—Kai Martius
Chief Technical Officer,
secunet Security Networks AG

SecuStack Use Case: Confidential Multi-party Computing

SecuStack uses the SCONE platform and Intel® Software Guard Extensions (Intel® SGX) for novel applications in the cloud. These applications include machine learning and multi-party computing. Some of SecuStack's Health and Life Sciences customers are using SecuStack to protect machine-learning models for transferring and processing patient data for confidential federated machine learning applications. It doesn't matter if the cloud service provider (CSP) is "trusted" or not—the training data, the code and the models stay protected from access by the CSP. SecuStack is powering extended research, which could potentially lead to exciting breakthroughs in diagnosis and treatment of disease.

Collaboration Helps Improve Cloud Security

Like Intel, secunet believes that real security cannot be achieved by software or hardware alone. Real security results from combining software and hardware features. For decades, Intel has been improving hardware security features such as secure boot and on-processor virtualization. Intel SGX adds important security features, including enclaves, attestation, memory encryption and protection of data in use. SecuStack takes advantage of all these innovations from Intel, combining them with a security-hardened version of OpenStack. The two companies have collaborated with Scontain, which has added several tools to its SCONE platform that utilize Intel SGX. The cooperation between all three companies has resulted in a verifiable, operable cloud OS that can finally bring cloud computing to use cases such as healthcare, banking, multi-party computation, confidential computing and the public sector.

During the development of SecuStack, Intel provided educational resources to SecuStack developers so they could understand what new Intel technologies were on the horizon. Intel engineers shared insights about how to use enclave technology for machine learning and artificial intelligence (AI) use cases, and answered questions about Intel SGX. Intel also provided early access to hardware offerings and remote access to Intel Labs and technology. Intel and secunet are looking forward to ongoing collaboration and investment in new technologies to further enhance cloud computing security.

SecuStack Use Case: Anonymization and Pseudonymization of Video Data in the Cloud

One of SecuStack's customers is using the security-hardened operating system for federated learning of artificial intelligence (AI) models by combining data from different sources, while remaining compliant with the General Data Protection Regulation (GDPR). This customer particularly values SecuStack's provisioning of complete lifecycle management of the customized secure cloud infrastructure. The infrastructure management can extend to managed Kubernetes clusters through services provided by SecuStack partner Cloud&Heat, to support machine-learning development. Other SecuStack features that provide business benefit to this customer include security-enabled virtual private network (VPN) connections that serve to better secure access to data and the ability to securely store and analyze video data without violating European Union data protection standards.

"We have an outstanding relationship with Intel, which provides information about upcoming technologies and engineering support. It's important to understand the technology—and its limits—to know how to use it and build a solid solution."

—Kai Martius
Chief Technical Officer,
secunet Security Networks AG

Spotlight on secunet Security Networks AG

secunet Security Networks AG is Germany's leading cyber security company. secunet employs more than 700 experts who strengthen the digital sovereignty of governments, businesses and society. The company offers a combination of products and consulting services, robust digital infrastructures and the highest level of security for data, applications and digital identities. secunet specializes in areas with unique security requirements, like the cloud, Industrial Internet of Things (IIoT), machine learning and eHealth. secunet's customers include German federal ministries, national and international organizations and more than 20 DAX-listed corporations.

Solution Ingredients

- **SecuStack cloud OS**
- **Scontain SCONE platform**
- **Intel® Software Guard Extensions (Intel® SGX)**
- **Intel® Advanced Encryption Standard – New Instructions (Intel® AES-NI)**
- **Cloud&Heat Managed Kubernetes**

Find the solution that is right for your organization. Contact your Intel representative or visit **intel.com/csp**

intel®

[1] https://www.intel.com/content/www/us/en/cloud-computing/deployment-models.html