Senonetwork Cloud Infrastructure

Overview

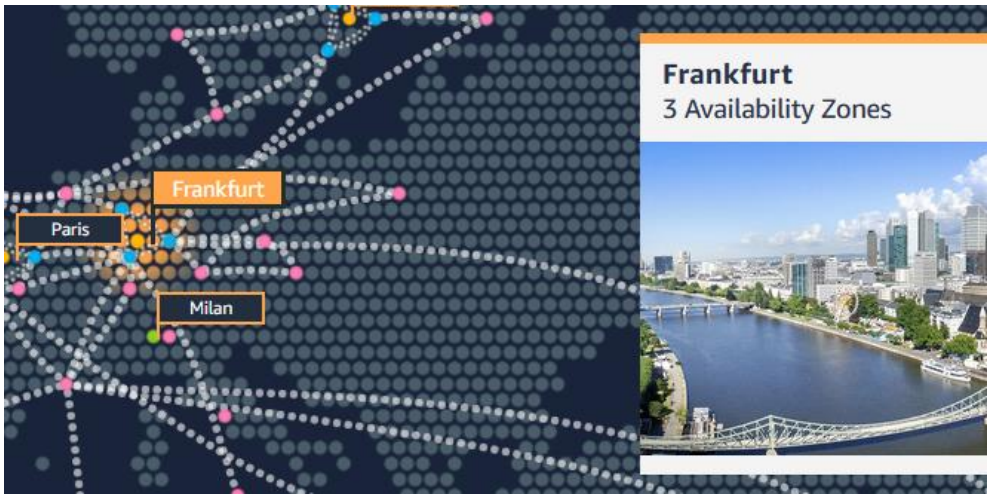
Senonet is hosted in the Amazon's cloud, called AWS (Amazon Web Services). AWS holds a huge number of certifications, e.g. HIPAA and ISO 27001. The complete list is available at http://aws.amazon.com/compliance/.

The AWS Cloud spans 69 Availability Zones within 22 geographic regions around the world https://www.infrastructure.aws/.

Each Availability Zone is a cluster of datacenters for fault tolerance and low latency. Availability Zones are connected to each other with fast, private fiber-optic networking, enabling you to easily architect applications that automatically fail-over between Availability Zones without interruption.

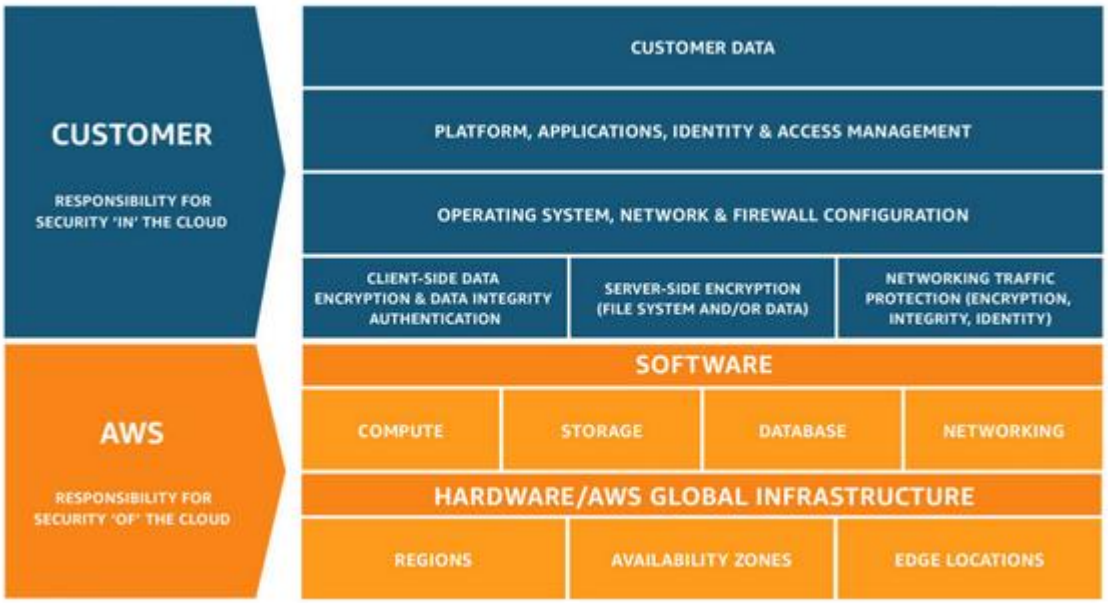
To increase control and flexibility AWS makes available Virtual Private Cloud (VPC) to its customer. VPCs lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

Senonet is hosted in Frankfurt, Germany, in a dedicated VPC.



Security

Security and Compliance is a shared responsibility between AWS and the user (or customer). This shared model can help relieve user's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall. The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment. As shown in the chart below, this differentiation of responsibility is commonly referred to as Security “of” the Cloud versus Security “in” the Cloud.



Within such a model, AWS provides security of the infrastructure and cloud services, while the partners are in charge of the custom software and data.

Main services used by Senonet

EC2 —Virtual Machine for computation

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. Amazon EC2's simple web service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment. Amazon EC2 works in conjunction with Amazon VPC to provide security and robust networking functionality for your compute resources.

S3 —Amazon Simple Storage Service (Amazon S3)

S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. Amazon S3 provides easy-to-use management features so you can organize your data and configure finely-tuned access controls to meet your specific business, organizational, and compliance requirements. Amazon S3 is designed for 99.999999999% (11 9's) of durability, and stores data for millions of applications for companies all around the world.

Amazon S3 maintains compliance programs, such as PCI-DSS, HIPAA/HITECH, FedRAMP, EU Data Protection Directive, and FISMA, to help partners meet regulatory requirements.

VPC —Virtual Private Cloud

Amazon VPC allows to organize EC2 machines and storage in virtual network and control access to the computational resources. VPC provides advanced security features, such as security groups and network access control lists, to enable inbound and outbound filtering at the instance level and subnet level. In addition.

IAM –Identity and Access Management

AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

IAM enables security best practices by allowing you to grant unique security credentials to users and groups to specify which AWS service APIs and resources they can access. IAM is secure by default; users have no access to AWS resources until permissions are explicitly granted.

More content on AWS

Certifications	http://aws.amazon.com/compliance/
	http://aws.amazon.com/compliance/aws-whitepapers/
Security	http://aws.amazon.com/security/
	http://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf
GDPR	https://aws.amazon.com/it/compliance/gdpr-center/
S3	http://aws.amazon.com/s3/
EC2	https://aws.amazon.com/ec2/
VPC	http://aws.amazon.com/vpc/
IAM	https://aws.amazon.com/iam/