Cloud

Sectra One

A fully managed Software-as-a-Service

SECTRA

Benefit from smooth upgrades, continuous maintenance, and scalability

Sectra One Cloud is a fully managed SaaS intended to eliminate an on-premises installation and provide users smooth upgrades, continuous maintenance, and a scalable solution—all in the cloud.

Sectra takes full responsibility to ensure there is enough computing power and storage resources to quickly display images, instantly return search results, and access the tools you need for efficient workflows. You connect to the service via Microsoft Azure ExpressRoute which will ensure stability and performance. Sectra will handle the migration process for your data.

Uptime to meet critical operations

Sectra guarantees an uptime of 99.99% (Monthly Uptime) to support your critical operations with E3-E4 subscriptions. E1-E2 subscriptions guarantee an uptime of 99.90%.

Frequent upgrades with minimal disturbance

You will gain access to the latest upgrades and features with little to no disturbance in your daily operations. Upgrade your system with minimal planned downtime through redundancy in the cloud.

Continuously maintaining the service

Sectra continuously monitors and maintains the service 24/7. To ensure the highest quality we run activities such as:

- High availability testing
- OS patching/updates
- Security and vulnerability assessment
- Certificate management
- Sectra SW upgrades
- Storage growth monitoring
- Resource utilization monitoring

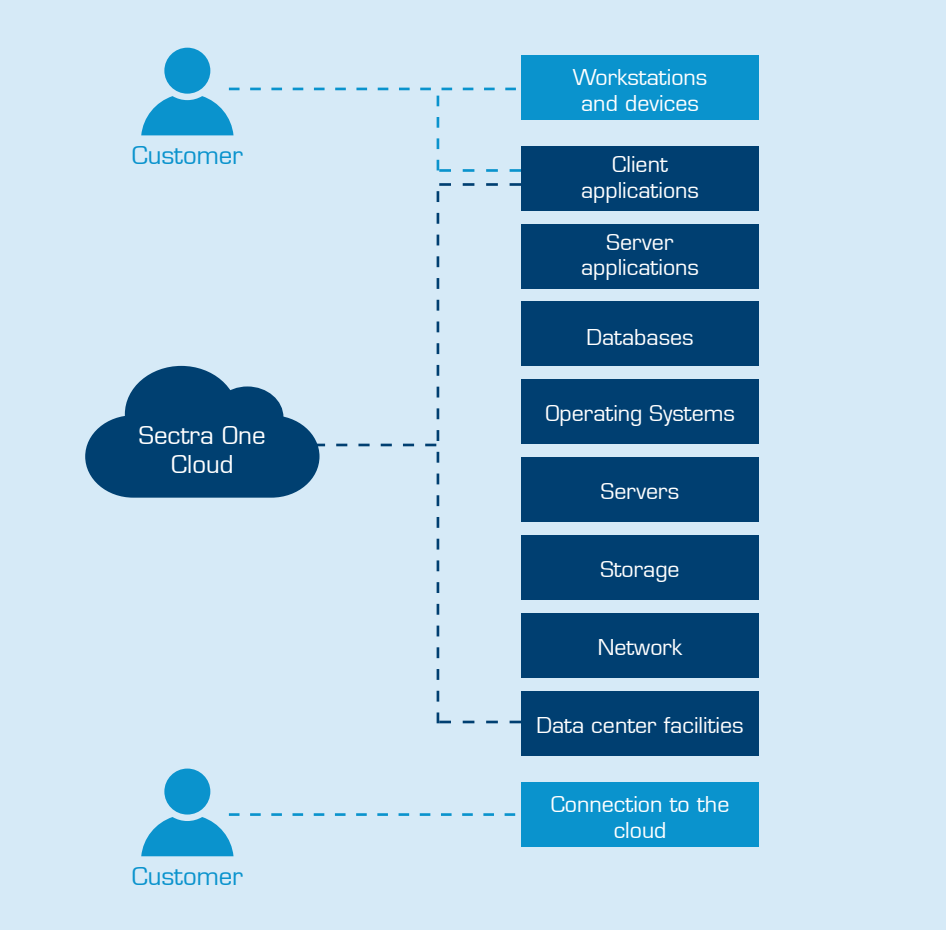
Planned maintenance is performed monthly with minimal to no impact on your operations.

Successful transition with experienced migration services

Based on Sectra's experience and expertise of migrating data from different systems, we provide flexible migration services to make sure your data is available in an efficient, quick, and secure way.

Clear division of responsibilities

You are responsible for the connection to the service and all the devices and their software needed for using Sectra One Cloud. Sectra is responsible for all the needed resources in the cloud to provide you with the service.



A multi-layered cloud security protects against cybersecurity threats

Security is an integral part of Sectra One Cloud. With our roots in cybersecurity at the defense leveland our assets for confidentiality, integrity, and availability of products and services, we protect your data.

The Sectra Cloud Security framework, a multi-layered security strategy, and our own team of dedicated cloud specialists continuously monitor the system and are ready to act when needed.

Strong governance and risk management to continuously secure content

Communication, data storage, integrations, operations, and documentation of the service is in accordance with applicable information security laws. All information remains within our control. You own the data you produce, and you decide which users have access to it and choose to migrate it in the event of termination of service.

Building and maintaining secure applications

Application security is an integral part of our development process. Sectra performs code reviews, vulnerability testing, and penetration testing on a regular basis.

Certified, HIPAA, and GDPR compliant

Sectra is ISO27001 (information security) and ISO27017/18 (cloud security) certified, as well as HIPAA and GDPR compliant, which permeates all our cloud operations. Our staff are all trained annually in security awareness, GDPR and HIPAA. We have several dedicated roles in the security field, Cloud Security Architect, Security Architect, and CISO.

Secure storage, compute, and transmission

We take actions to secure data protection and privacy including encryption of client network traffic. Information is stored in redundant storage systems and access is protected with strong access control. Operation of the service takes place on redundant hardware in data centers with Microsoft's high security.

Top-class secure Microsoft datacenters

Microsoft datacenters strictly control physical access to the areas where your data is stored. Microsoft has an entire division devoted to maintaining state-of-the-art physical security by designing, building, and operating the physical facilities where our solution runs in Microsoft Azure.

Secure operations through knowledge, processes, and technology

Sectra achieves high operational security in our cloud services by applying several best practices and security solutions:

- Strict identification and access management
- Regular patching on all levels
- Routines for acting on security incidents
- Vulnerability scanning and penetration tests
- Threat detection with anti-virus software
- Hardening systems
- Best practice configuration
- System and application logging

Isolation and layered defense architecture

Security is achieved through a combination of Microsoft Azure's and Sectra's network security in the virtualized environments. Strong isolation between customer systems ensures no possible leakage between customer data sets. A layered defense architecture by segmentation within each customer system protects stored data and components processing data. Network monitoring is used to both detect and trace any suspicious activity, and to ensure network security.

Minimizing impact of incidents through redundant design and scalability

When designing the software and the underlying cloud infrastructure Sectra's focus is to create a reliable service. Our SaaS is available 24/7, with a minimal need for service windows. We achieve this high availability with a scalable solution design. To prevent incidents, we monitor vital data of servers and user devices and potential disasters are covered by backups and a recovery task force.

Sectra One Cloud avoids problems by utilizing a combination of functionality from Microsoft Azure and Sectra to create a solution that has the highest possible availability. Multiple Azure Availability Zones and instant fail over mechanisms keep your data protected. The solution minimizes impact in the event of a disaster, involving failure of a data center.

Replication of data reduces traditional backups

Sectra uses Microsoft Azure Availability Zones to secure backups and replicate copies of images. These zones are stretched across multiple data centers making data available in the case any of the zones are lost. Full backups of databases run every day and weekly. In case of a disaster, we have minimized the data loss to a maximum of ten minutes. We test backups regularly to make sure our restore procedures work appropriately.

Extensive procedures and automatic failovers

Sectra also uses Microsoft Azure Availability Zones for extensive procedures and automatic failovers. These procedures are regularly reviewed by external ISO audits and tested for their effectiveness. Critical parts of the solution are redundantly implemented. If a disaster occurs in one Azure Availability Zone, the service is automatically kept online by another zone. To restore service redundancy, deployment scripts and backups are used to quickly get the service back online in the affected zone.

Foresee incidents to ensure stable operations

Sectra Monitoring watches over system services all the way down to the operating system level. An alert will occur if threshold values are exceeded, and a monthly system report is created where the monitored system's operational quality is clarified. The service alarms to proactively prevent downtime and poor performance.

Fast access to images and reliable performance over time

In conjunction with Microsoft, Sectra has developed a solid architecture, using Azure's proven and high performing components that are optimal for our software. A continuous optimization is happening, behind the scenes, based on your specific usage of the service.

Utilizing the latest cloud storage technology means immediate access to current and prior content

Fast access to new images and priors is achieved with a high-performance image cache and by using streaming technology for archived data.

Sectra One Cloud manages variations in network performance

The software layer is designed and developed to manage different connectivity characteristics, such as latency, towards end user workstations.

Connect to the service

Connecting to the service via Microsoft Azure ExpressRoute secures high performance connectivity. It has the best prerequisites for stability and performance.

We help you decide how to connect

Together we choose redundancy and adequate bandwidth for your connection and you extend your on-premises networks into the Azure cloud over a private connection with the help of a connectivity provider. Sectra will assist you with connection requirements and with testing and validation when connecting.

Maximizing the availability and performance of clients and devices

Azure Monitor is used when managing the solution, and to drill down on alerts from Sectra Monitoring. It maximizes the availability and performance of clients. It is a comprehensive solution for collecting, analyzing, and acting on telemetry from the cloud environments. Its information helps us understand how the applications are performing and proactively identify issues affecting them and the resources they depend on.

SECTRA

Sectra AB • info.medical@sectra.com • medical.sectra.com