Whitepaper

Cybersecurity in Sectra One Cloud

Defending against ransomware in today's complex threat landscape

In today's complex threat environment, everyone with an Internet connection is a target for cyberattacks, especially for businesses operating within the healthcare sector. Therefore, to remain operational, companies must assume that they are defending against highly skilled actors, which means their organizations must have an exceedingly high-security maturity and advanced security controls. Furthermore, organizations must remain focused; they must focus on their core mission and invest their resources wisely to advance that mission. They must carefully choose partners whose core mission supports their own.

Utilizing a strategy like this will provide several key benefits from a security perspective:

- **Internal IT (Information Technology) burden and resource constraints relief.**
  Internal security resources can focus on protecting the core business.
- **State of the art security solutions.**
  Utilizing the economies of scale offered by the SaaS (Software as a Service) delivery model will enable the care provider to benefit from investments in security, redundancy, and resiliency made by the SaaS providers and Cloud Service Providers (CSP).
- **Cost-effective security operations.**
  Continuing to utilize the economies of scale achieved by consolidation, but more importantly, effectively using the Product Vendor/SaaS provider's expertise in operating and securing products they know intimately.

SECTRA

Knowledge and passion

The threat landscape is more complex than ever

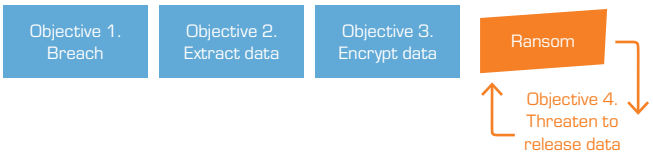
The threat landscape that we operate in today is more complex than ever. A significant reason for this is that the lines between cybercriminals, organized crime, and Nation-States are becoming increasingly blurred. It is becoming much harder to know who your adversary is. Five years ago, TTPs (Tactics, Techniques, and Procedures) were only utilized by nation-states, but today TTPs are being used against civilian targets by cybercriminals and organized crime with the sole motivation of extorting money from their victim. We also see nation-states using their advanced capabilities and engaging in industrial espionage against civilian enterprises in parallel. Today, everyone is a target. Even if your organization is not the direct target, you risk becoming collateral damage in cyberattacks against others.

Threat actors are not becoming more sophisticated, but their business models are. What used to be pranks or skill challenges have turned into multi-million dollar businesses that are operated as such. The criminal elements of today are often very sophisticated operationally, where different actors specialize in specific tasks in the breach chain and sell their output to the next actor in the chain. Threat actors are also becoming much faster. The time needed from their initial access to achieving the objective (e.g., encrypting your data) has decreased from days or weeks to typically less than 24 hours.

Clear trends point to the fact that more breaches are occurring due to software vulnerabilities instead of the more traditional threat vectors such as social engineering (e.g., phishing or spear phishing). The challenge for healthcare providers is that this attack vector enables automation for the attackers. Cyberattacks are being automated to target a wide array of companies with an insignificant extra cost for the adversary.

This allows the threat actors to develop their business model further to include scalability. Instead of developing a tool and manually deploying it, it is becoming increasingly normal that some threat actors sell their tools and exploits on the dark web, often complete with deployment and usage documentation at a low cost. Many threat actors of today do not need to have the skills to develop advanced exploits themselves as they buy them often packaged as a service. We have seen Distributed Denial of Service attacks offered as a Service (DDoSaaS), and in more recent years, Ransomware as a Service (RaaS) is becoming the norm. These services are heavily automated, so they can easily be deployed against a wide range of targets by perpetrators that do not have the expert competence.

One of the most severe threats that has emerged is the threat of double extortion. As the name implies, double extortion is a modus operandi (M.O.) where the criminals try to ransom their victims twice. After initial access, the criminal extracts data from the breached IT system before they deploy the ransomware. The next step is to demand payment to release the encryption keys to the victim, and if the victim pays for the keys, the criminal now demands payment not to release the stolen data to the public.



Interestingly, with this M.O., the criminal must make a business decision on how to maximize their profits. The group can either give the keys to the victim after payment and move on to the next victim or try to maximize profit through double extortion. They must weigh the possible return of a successful double extortion against the risk that their reputation will become one as always requiring more than one ransom, thus making the victim less enticed to pay.

This threat environment is naturally also affecting the healthcare sector. Unfortunately, the healthcare sector has been a soft target for cybercriminals. The fact that actors within healthcare must have an absolute focus remaining operational to provide care for their patients is a major reason for this. Several organizations within the industry have crypto wallets with funds so they can quickly pay ransom in the event of a cyberattack. Further, the threat of double extortion is grave to enterprises operating under strict regulatory requirements. This makes healthcare providers even more enticed to pay ransom to try and avoid penalties and the legal aftermath of a breach.

How do you ensure uninterrupted operation in a complex threat landscape?

To excel within today's complex threat environment, companies must focus on their core mission. No individual company can do it alone and come away with an acceptable level of risk or acceptable level of cost because there is too much complexity involved. Businesses must focus on their core mission and invest their resources into doing that as best as possible. To handle the necessary dependencies for your core mission, you must choose partners whose core mission supports your own. This way, you allow every actor in the chain to focus on what they do best. This leads us to a SaaS delivery model.

Take enterprise imaging as an example. In this case, we have a healthcare provider whose core mission is to provide state-of-the-art healthcare to their patients. For this, tools are needed, and enterprise imaging is a crucial tool within this environment.

The healthcare provider can procure this tool by turning to an enterprise imaging provider and letting them focus on providing customers with state-of-the-art enterprise imaging software as a service. This provider knows their product intimately, down to every single line of code. This means that they have a unique perspective and position when operating, maintaining, and securing the service.

As a SaaS provider, they can focus on this by choosing to partner with a strong Cloud Service Provider as they can provide a state-of-the-art platform to operate on. A strong CSP will offer physical security, redundancy, and resiliency at levels that most companies do not have the capacity or budget for.

In this scenario, every entity is focused on what they are best at; the customer is focused on their core mission, the enterprise imaging provider is focused on securing, patching, maintaining, and operating their application, and the cloud service provider is focused on providing a rock-solid platform. With everyone focusing on their core missions and expertise, it is possible to achieve an economy of scale in building a mature and secure environment.

It is worth remembering that security has several aspects to it. The most common aspect that is thought of first is keeping the data confidential, which is crucial when handling healthcare information. We argue that the availability of that data is equally important. The CSP's data redundancy in the cloud is something a single medical practice cannot compete with at a reasonable cost.

In summary, operating a solution in the cloud will help you stay operational and more secure in the case of enterprise imaging because:

- Each party can focus on their expertise and provide the best possible deliverables.
- A SaaS delivery model allows for economies of scale regarding operational and security measures being correctly configured, monitored, and maintained. This means that healthcare providers get relief from IT burden and internal resource constraints.
- The cloud service provider can offer data redundancy and resiliency solutions that are cost-prohibitive to build and maintain on-premises for the healthcare provider.

Cybersecurity in Sectra One Cloud

Although the threat landscape has become significantly more complex, defending against these modern threats boils down to well-proven security best practices.

At Sectra, we do not view security as just technology. Our perspective is that several different security aspects must be leveraged to reach the high-security maturity necessary to operate in the harsh threat landscape of today.

For this reason, security in Sectra One Cloud is built utilizing the following aspects:

Leadership

Security starts at the management level of any organization. Security must be a topic of discussion in the boardroom at a strategic level down to the management teams running the day-to-day tactical operations of the business. Management must create and maintain security policies, metrics, and goals that the organization can work towards and be willing to commit monetary and human resources to reaching these goals. Security thrives inside an organization when management demonstrates their dedication to a secure operating environment.

Sectra is ISO27001, 27017, and 27018 certified and the Cloud Security Alliance's STAR level 2 certification is pending which demonstrates Sectra's strong commitment to maintaining a strong and healthy security posture, not only in our products, but also in our daily operations.

Dedicated people

A factor of security that is often overlooked are the people inside an organization. If an organization does not have well-trained and well-motivated staff, it does not matter how much management has invested in technical controls, security will suffer.

Sectra One Cloud is operated and delivered by the best people in the business who have a passion for customer satisfaction that drives them to be a little better every day. At Sectra, not every employee is a cybersecurity expert, but everyone is aware of relevant security risks for their position and duties. At Sectra, every employee takes the confidence our customers show us when entrusting us with their data very seriously. Security awareness training results in that everyone working with Sectra One Cloud understands the absolute need for strictly following policies, procedures, and checklists. Sectra has built a healthy security environment where all employees are encouraged to provide feedback to improve our security posture.

Best practices and procedures

Maintaining a strong security posture requires a clear structure in place for how the organization works with security. An organization must implement a cybersecurity program that encompasses the entire organization.

Operating within the current threat landscape, you are required to shift from a defensive mindset of "prevent breach" to an "assume breach" mindset. Since the threat landscape has changed towards exploiting new software vulnerabilities and being able to react to upcoming potential breaches, the "assume breach" mindset is a must. An "assume breach" approach focuses on detection and incident response rather than on perfect preventive technical controls, which do not exist. Of course preventive measures must always be in place; no business will ever succeed by not implementing them. Preventive controls such as patching are crucial in withstanding threats from vulnerabilities in software.

Sectra has developed a tactical cybersecurity program that rests on four pillars: *protect, detect, respond, and review.* This cybersecurity program is utilized to protect the Sectra One Cloud service. On top of this, customers utilizing our cloud service are given access to Sectra's One Cloud are given access to Sectra's award winning support. Every support ticket is handled by Sectra's dedicated and highly skilled in-house support teams. No support is outsourced to third party providers which guarantees full control with the best quality and which minimizes the risks of supply chain attacks.

Technology

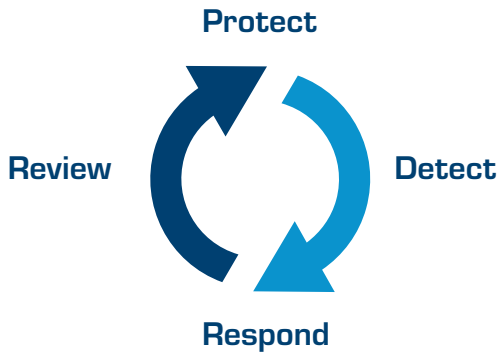
Technical security architecture and controls are an important part of the overall security posture of any system or service. Sectra One Cloud is designed with the security of the data managed by the service as a priority including an architecture that promotes security from the initial design. Sectra's system and cloud architects work together with architects and experts from Microsoft to ensure that Sectra One Cloud leverages the most effective security features in Azure. All deployed servers and components within a Sectra One Cloud tenant are hardened using industry standards and best practices to limit exposures, and in the event of a breach, limiting the ability for lateral movement.

Sectra utilizes a multi-layered approach to secure Sectra One Cloud where technical controls are just one aspect, and where leadership, people, and operations are equally as important.

Defending against ransomware in Sectra One Cloud

The first step in a ransomware attack is that a threat actor attempts to establish a foothold with malicious software (malware) in a system. This can be accomplished by exploiting software or system vulnerabilities, or with a social engineering type of attack (e.g., phishing). Before the malicious software becomes destructive, it will try to hide itself and disable backups and other tools that can aid in detection and restoration. After this, the malicious software starts encrypting critical files and requesting ransom to unlock the system again. It is also common that the malicious software exfiltrates data from the system, and that the threat actor uses this stolen data for cyber extortion.

Protecting against the modern ransomware threat requires not only technical controls but ensuring that several aspects of cybersecurity are deployed. This is most effectively done by defining a cybersecurity program and at Sectra we have defined our cybersecurity program around the four pillars *protect, detect, respond,* and *review*.



"Protect" is focused on preventing or blocking any steps in the breach chain. This is accomplished in Sectra One Cloud by combining a sound security architecture with a defense-in-depth approach, which ensures that a breach of one security mechanism does not result in a breach of the entire system. Best practice technical controls are also deployed throughout the environment in a defense-in-depth approach.

"Detect" is about detecting any odd or irregular events in the system. As the complexity of modern threats are increasing, protecting a system is not enough. You must have the ability to detect irregular behavior so that you can deploy effective incident response activities. Detection capabilities can also be utilized to achieve something referred to as virtual patching. Virtual patching is the practice of detecting Indicators of Compromise (IoCs) for specific vulnerabilities during the time gap between the release of a patch and when the patch can be applied to production systems. This will allow for thorough functionality and stability testing prior to deployment in production, meanwhile still having visibility and awareness if the vulnerability is targeted by attackers in a breach attempt. In Sectra One Cloud, detection is implemented by combining cloud native detection features together with in-house developed tools and procedures. Threat intelligence is also used to augment the detection ability. If an anomaly is detected or a breach is suspected, resources within the "Respond" pillar are dispatched to evaluate the situation and triage the breach.

Finally, as the threats are continuously evolving, so must the deployed defensive techniques. This is where "Review" comes into play. All techniques, procedures and tools must be regularly reviewed and improved.

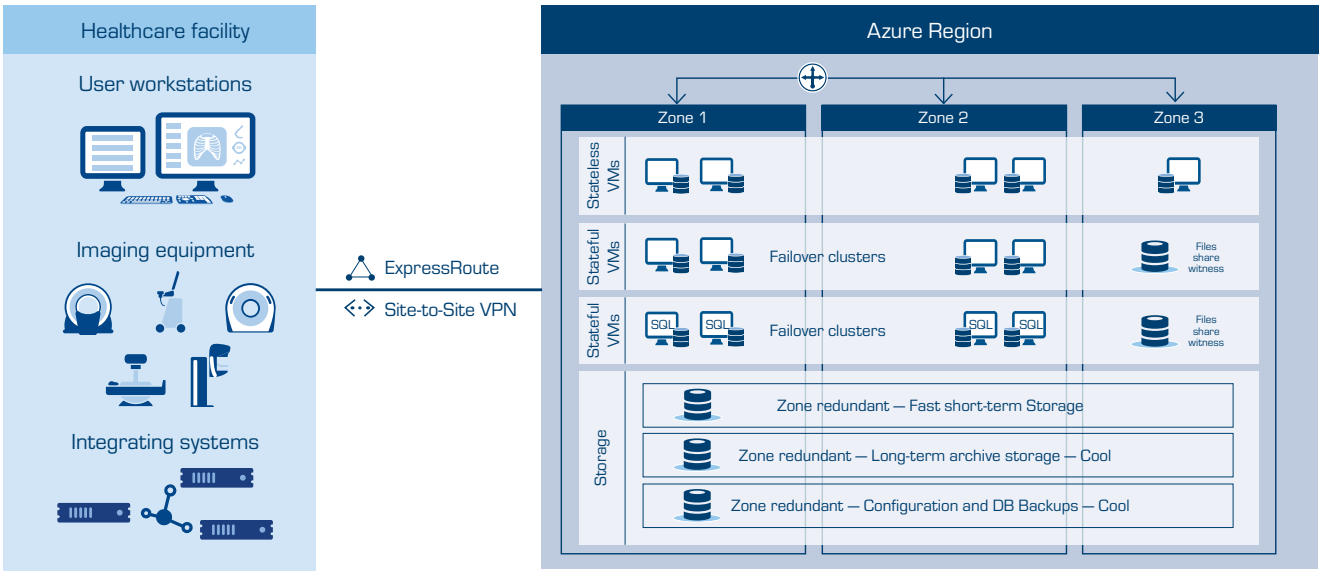
Protect

The system components within Sectra One Cloud are protected against malicious software (malware) in several security layers. Physical and virtual access to the system is protected by high levels of physical security and strict firewall rulesets. All engineers that have access to the system are trained in IT security awareness and follow strict policies on what activities and software are allowed in the system. The system is continuously monitored for vulnerabilities and updates are applied on a regular cadence.

All components that are deployed as part of the system are designed to minimize exposure and the risk of potential vulnerabilities in the system. Antimalware is an integral defensive layer of the system to minimize the risk of malicious software being installed.

To minimize impact and to ensure the ability to restore the system in case of an attack, the solution design includes segmentation with a high level of redundancy. By having segmentation, an attack would be limited so that the affected part of the system can be restored while the other segment provides the service without any interruptions.

To add more protection, everything that gets stored in a Sectra One Cloud tenant is automatically and synchronously replicated to two separate data centers. There is no extra software or configuration required and is built in by design. Any services accessing the data can access the data from any location, and in the case of a zone outage, all data is persisted in multiple places. This includes databases, short-term storage, and long-term archive data.



Detect

For a ransomware attack, it is often possible to detect the initial steps of the intrusion before the ransomware attack is executed. Our service design includes security logging that tracks activities and raises alerts when suspicious activities are detected. For ransomware, there are known indicators that can be used to detect an attempt before the attack is executed.

Respond

When a suspicious activity is detected or a system failure indicates that a ransomware attack is imminent or underway, there are formal procedures documented on what actions to take. Sectra has internal IT security specialists and incident responders trained to be able to determine what actions are needed to stop the activities and restore the system. These specialists form a Security Incident Response Team (SIRT) which reports to executive security management.

Sectra deploys standard security tools to triage the system in the case of a breach. Security logging is an important layer for response activities. This enables Sectra to determine what the root cause of the breach was and further enable us to remediate the point of attack and recover without the adversary being able to take over the system again.

The business continuity and disaster recovery plans include strategies on how to restore the system to full service and full redundancy after the initial response activities have been performed.

Review

Our strategies, personnel training, procedures, designs, and tools are all reviewed on a regular basis to ensure that our deployed systems are compliant with applicable standards. This is completed by internal and external party audits, frequent tabletop reviews, and technical reviews of deployed systems. This includes but is not limited to penetration tests and vulnerability scanning.

The above write-up is not only applicable for ransomware attacks, but for any type of IT security incident. With this in place, we are confident that Sectra will protect critical assets and that we are ready to act if an IT security incident occurs.

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

SECTRA
Knowledge and passion