SentrySuite® Software Product Security

Digital threats in pulmonology

SENTRYSUITE® SOFTWARE

vyaire™ MEDICAL

Cybercrime around the world

The number of cyberattacks increased by

60% compared to the previous year and

470% more patient records are affected. [1]

A SINGLE PATIENT RECORD can be worth up to

$1000 ! [2]

$ $ $

A cyberattack is costly to remediate and will cause ongoing revenue loss until resolved. [3]

It takes on average 16 days to recover from a ransomware attack. [4]

The risk of sensitive data

While diagnosing and treating a patient, a high amount of sensitive data may be gathered and stored without taking any special precautions. The use of modern diagnostic devices is even increasing this number of data and integrating different diagnosis devices with each other, while being indispensable for holistic diagnoses.

Patient data is very valuable on the black market, making medical care providers primary targets for hackers. Physicians are underestimating the potential of security issues which can cause regulatory and commercial impacts as well as the loss of reputation and loss of money.

16 days to recover your network from a ransomware attack

Imagine your lab is off for one day

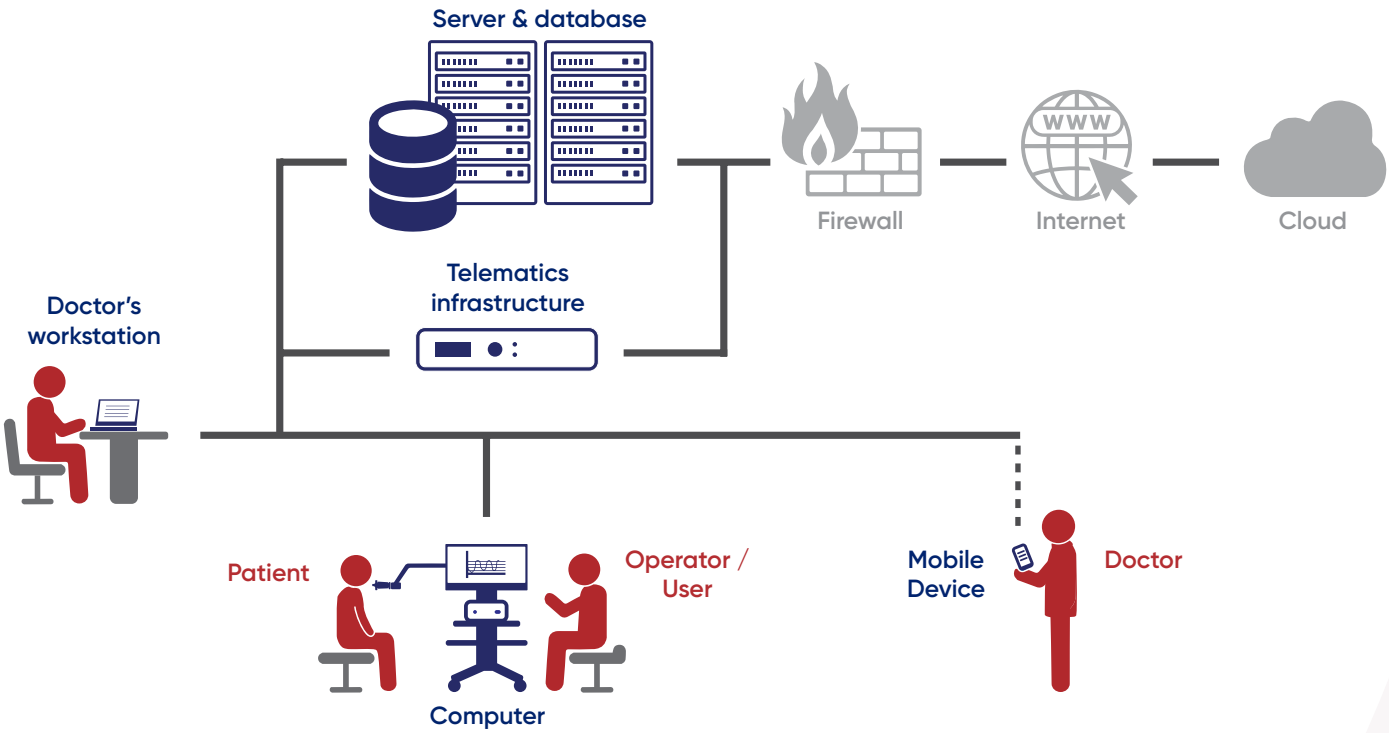
- You need to send all patients home
- Depending on the schedule of your latest data backup, you might lose data
- You lose patients & reputation

Leading to

- A risk to the health status of chronically ill patients
- A loss of reputation, loss of patients, loss of money
- Continued fixed costs without earnings
- Repeat lost patient diagnostic tests

The threat to your lab is real. Cyberattacks pose a risk to your patients' health and do have a tremendous impact on your business economics. Existing lab contingency insurances often do not cover in case of lab downtimes due to cyberattacks and IT experts often report difficulties while recovering the network.

Typical Lab Set-Up



Labs can only be as secure as their weakest part. Elements of a lab or network are not only the medical devices, computers, servers or mobile devices. Operators / users, physicians, patients as well as the network and IT infrastructure are critical elements of a secure lab.

It is important to find the right partners to create a continuously secure environment, no matter if it is just a standalone system or a whole networked lab with an online cloud connection.

The right questions for your med tech or IT supplier

As a secure lab is composed of different parts from different vendors, all decision makers need to be able to select the right partners. An understanding of potential hazards and threats within a typical lab set-up is helpful to be able to ask questions you can discuss with potential partners to understand their efforts in terms of product security.

Learn more about

- What is the hazard that you are facing?
- What are the threats that can arise from the hazard if not addressed?
- How Vyaire and SentrySuite Software address these hazards for you
- Questions that you can ask the vendor of your current solution

People may access sensitive data that they are not authorized to view or modify.

Sensitive data may be viewed, manipulated or stolen.

Vyaire SentrySuite supports individual accounts for each of your users. Accounts can be protected with strong passwords. You can define requirements for the complexity of the passwords to ensure that they meet your desired standard.

Furthermore, SentrySuite supports user authentication against an external user directory such as LDAP or Windows Active Directory to enable your users to use their existing accounts to log into our solution.

Does your solution support unique user accounts with strong passwords and an optional connection to an existing identity provider?

People may access sensitive data that they are not authorized to view or modify.

Sensitive data may be viewed, manipulated or stolen.

Vyaire SentrySuite supports assigning users to defined roles. You can either use existing roles that come preconfigured or customize or create new roles. Roles can have fine-grained access rights assigned to them so you can ensure that users only have access to information that they require to perform their given job.

Furthermore SentrySuite allows you to assign patient data in the solution to a location. You can e.g. create locations for each of your branch offices or labs. Patient data that is assigned to a location will only be shown to users which work at the given location. This ensures that you can separate patient data from different locations and only show users patient data that is relevant to where they work.

How does your product provide role-based access control to ensure users only have access to resources they require? Does it support different locations for larger organizations?

Application software and device software updates are not validated for authenticity before installation.

Attackers may tamper with software updates to compromise the security of the installed system. Unprotected devices enable attackers to facilitate cyberattacks - sensitive data may be viewed, manipulated or stolen.

Vyaire has added the possibility to check the integrity of the SentrySuite software installation sources and any updates that are provided. This helps you to ensure that you are installing software that is genuine and has not been tampered with.

Is the supplier able to check whether there installation discs are secure?

Devices are not kept up to date with the most recent security updates released by manufacturers.

Unprotected devices enable attackers to facilitate cyberattacks - sensitive data may be viewed, manipulated or stolen.

Security updates that were not validated by the manufacturer may cause issues upon installation which can render your devices inoperable until fixed.

Microsoft continually releases new security patches to address issues in its operation systems. Newly released security patches for the Windows 10 operating system are validated by Vyaire for compatibility with SentrySuite ususally within 4 weeks from release by Microsoft. The results of these compatibility tests are made available on the Vyaire Product Security website (www.vyaire.com/product-security).

Do you test new operating system security updates for compatibility? Is there a proposed timeframe? How are the test results shared with me?

Devices are not configured in line with best practises in order to provide maximum security for sensitive data.

Unprotected devices enable attackers to facilitate cyberattacks - sensitive data may be viewed, manipulated or stolen.

The Vyaire Product Security team together with SentrySuite Product Management has created a comprehensive SentrySuite Product Security Whitepaper. The whitepaper covers all aspects of product security and enables your IT partner to develop a professional understanding of how SentrySuite can integrate itself into your IT cybersecurity landscape. The whitepaper will be updated for every new major version of SentrySuite that will be released in the future.

Do you offer up-to-date system security guidance in written form?

Devices may contain security vulnerabilities that you or your IT partner are not aware of, posing an additional risk for your network.

Unprotected devices enable attackers to facilitate cyberattacks - sensitive data may be viewed, manipulated or stolen.

Vyaire is committed to a responsible disclosure process to inform customers about security issues in our products in a timely manner, depending on the severity and urgency of the issue discovered.

We will publish comprehensive information about potential security threats and issues and what you can do to address the potential risk for you organization on our Product Security website (www.vyaire.com/product-security).

Will you notify me of security issues in your product? How and how quickly?

Devices may contain security vulnerabilities that you or your IT partner are not aware of, posing an additional risk for your network.

Unprotected devices enable attackers to facilitate cyberattacks - sensitive data may be viewed, manipulated or stolen.

Vyaire performs monthly security scans of all SentrySuite versions that are supported in the market. Vyaire uses industry best practises and best-in-class tools to perform these scans. Scan results are audited and remediation of issues found is tracked and included in future software releases.

Do you perform regular security scans of your software (e.g. via Nessus Scanner)? How often?

Vendors may not be aware of security issues in their products and may not have appropriate resources to address the discovery, tracking and remediation of those issues.

Unprotected devices enable attackers to facilitate cyberattacks - sensitive data may be viewed, manipulated or stolen.

Vyaire has an Information Security team that directly reports to the Chief Information Security Officer. The team consists of 10 full-time security professionals and is grouped into a Product Security team and a Security Operations Center team.

How is the team composed that deals with cybersecurity in your organization?

Devices are not configured in line with best practises in order to provide maximum security for sensitive data.

Unprotected devices enable attackers to facilitate cyberattacks - sensitive data may be viewed, manipulated or stolen.

Vyaire is continously evaluating the security of 3rd party software components that are used in the development and operation of its SentrySuite software solution. As part of this effort, Vyaire has made a consicous decision to replace Adobe Reader, which is known for reoccurring high-severity security issues with another more secure solution which helps you to reduce your exposure to security threats.

Adobe Reader is known for reoccurring security issues. Does your product utilize Adobe Reader? If yes, have you ever evaluated more secure alternatives?

Sensitive data is stored without appropriate protection, e.g. encryption.

Unprotected devices enable attackers to facilitate cyberattacks - sensitive data may be viewed, manipulated or stolen.

Vyaire SentrySuite does not store any sensitive data (such as Personally Identifiable Information [PII] and/or Protected Health Information [PHI]) locally on client workstation PCs.

Sensitve data is stored exclusively in the central database located in the secure network backend in your data center.

SentrySuite fully supports encryption of hard drives on both client and network backend server via Microsoft Bitlocker. This ensures that sensitive data is encrypted in storage.

Does your solution store PHI/PII data locally despite of it is connected to a network server? If this is the case: Is local encryption of data (e.g. via Bitlocker) supported?

Application software and device software code is not validated during operation.

Attackers may tamper with installed software to compromise the security of the installed system. Unprotected devices enable attackers to facilitate cyberattacks - sensitive data may be viewed, manipulated or stolen.

Vyaire utilizes digital signatures for all application files that contain executable code. This digital signature helps any anti-virus or anti-malware system that you are using to establish the authenticity of the application files. It is proof that the file signed has been created and distributed by Vyaire Medical and is authentic.

Are the software libraries of your products are protected by digital signatures?

Sensitive data is not appropriately anonymized before it is shared with a third party which should not have access to sensitive data.

Third parties may gain access to sensitive data that they are not entitled to.

SentrySuite allows you to anonymize exported data before you share it with us or any other third party. This helps you to comply with applicable data protection regulations to ensure that your patients' sensitive data stays protected and is not shared with unauthorized third parties.

Is there a way to exchange patient and measurement data or send to Service organization in case of an inquiry? Can this data be anonymized to guarantee confidentiality of data?

Connections to information systems may not be monitored for unauthorized attempts from the network.

Attackers that manage to enter your network may remain undetected while trying to connect to information systems to gain access to sensitive data.

The SentrySuite network backend continously monitors all connections that are attempted and recognizes if a connection attempt is not authorized. SentrySuite will document unauthorized attempts for further review and analysis when you require additional information on possible security issues in your environment.

Has your software possibilities to detect unauthorized connections (intrusion detection system)?

Sensitive data is transferred over your network without any protection.

Attackers that manage to enter your network can easily capture unprotected data while it is transferred from system to system without having to gain deeper access into your systems.

SentrySuite supports full encryption of all data that is transferred between the SentrySuite client systems and the SentrySuite network backend. Encryption is facilitated using industry standard encryption methods while adhering to encryption best practises.

Does your product support encryption of sensitive data that is transferred over my network?

REFERENCES

1. https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/
2. https://www.beckershospitalreview.com/cybersecurity/patient-medical-records-sell-for-1k-on-dark-web.html
3. https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/
4. https://www.zdnet.com/article/ransomware-attacks-are-causing-more-downtime-than-ever-before/

GLOBAL HEADQUARTERS
Vyaire Medical
26125 N. Riverwoods Blvd.
Mettawa, IL 60045
USA

Vyaire Medical GmbH
Leibnizstrasse 7
97204 Hoechberg
Germany

CE 0123

vyaire™ MEDICAL