Telefónica Tech

This report is offered by celcom business

NextDefense

Cyber Security for *Healthcare*

1

Introduction

2

Cyber security for Healthcare

- The environment
- Security weaknesses
- ENISA security recommendations

3

Telefónica Tech's proposal for Healthcare

- Processes
- Technologies
- Management

Executive Summary

In the era of digital transformation, the number of devices deployed and their digital interconnections are the key to improving operational and administrative processes related to patient treatment and management. However, in healthcare, cyber risk is a daily reality regarding these devices and their exposure through communication networks.

Healthcare executives face a real problem: Is it worth investing in new technologies that will help optimise processes while putting the users and/or systems of my hospital's infrastructure at risk?

Investment in new technologies is not at its peak since managers are not confident that they have a secure environment in which to deploy them. Worse still, decisions are sometimes made without knowing the consequences, for example, of having a system vulnerable to cyber-attacks that could compromise the entire hospital's operation, from its information systems to its instrumentation or imaging equipment.

In the digital times we live in, it is not an option to refuse interconnecting. However, it must be done with guarantees of protection against cyber-attacks.

Telefónica Tech has been providing cyber security solutions to clients in healthcare since the beginning of its digitalisation, enabling them to invest in new technologies without increasing the risk of cyber-attacks. Telefónica's footprint currently extends around the world, offering specialised solutions and services to minimise cyber security risks in healthcare centres and devices.

This document presents in an accessible, graphic and representative way the need to deploy cyber security solutions and services in healthcare, as well as Telefónica Tech's proposal to minimise cyber security risks. Firstly, the main actors that coexist in the healthcare ecosystem are analysed. Afterwards, we explain the three main pillars of our proposal through which our clients can protect their infrastructures.

1 Introduction

The digital transformation and the interconnection with devices, equipment and infrastructures in healthcare enable different opportunities for the new generation of hospitals. In this context, The European Union Agency for Cybersecurity (ENISA) presents a number of key objectives that can be achieved with new technologies. The main ones are:

- **Improved diagnostics:** Improving and detecting the best treatment methods for patients by information mining.
- **Continuous flow of patients:** Optimisation of administrative processes and patient flow, reducing waiting times.
- **Remote healthcare:** Monitoring patients remotely using IoT devices.

The opportunities presented by new technologies and interconnectivity not only benefit patients and healthcare staff: the exposure of any healthcare asset to communication networks, both internal and external, increases the chances of cybercriminals to successfully execute attacks.

Although there is not total transparency on cyber-attacks on healthcare at a global level, we highlight the following cases, all in 2020 and in different geolocations, which exemplify the impact of cybercrime in this sector:

JANUARY 2020
Hospital in Madrid, Ransomware, no access to medical records, manual paper operation.

MARCH 2020
Hospital in the Czech Republic, Ransomware, network down, all computers down, operations delayed.

MAY 2020
European Group, ransomware, operational problems.

SEPTEMBER 2020
A critically patient did not make it to the hospital in Wuppertal alive, where she had to be transferred due to the collapse of services caused by a ransomware attack at the Düsseldorf University Hospital.

OCTOBER 2020
Hospitals in Florida: Ransomware, 1 million medical records stolen.

NOVEMBER 2020
Seattle clinic, security breach, online payment data theft.

The impact of cyber-attacks on healthcare can be seen in a number of different areas, for example:

Economy:
Ransom payments for encrypted data, the repair or replacement of affected systems, or the shutdown of hospitals, cause an overall economic
cost of hundreds of millions of euros per year.

Reputation:
Hospitals, as well as public and private organisations, have their reputation affected by any public incident.

Well-being:
Congestion in waiting rooms, administrative delays, logistical problems or the shutdown of mobile applications are examples of direct impacts on the well-being and comfort of users of hospital systems and infrastructures due to cyber-attacks.

Sensitive information:
Information theft can result in the uncontrolled disclosure of confidential and sensitive patient and health infrastructure information.

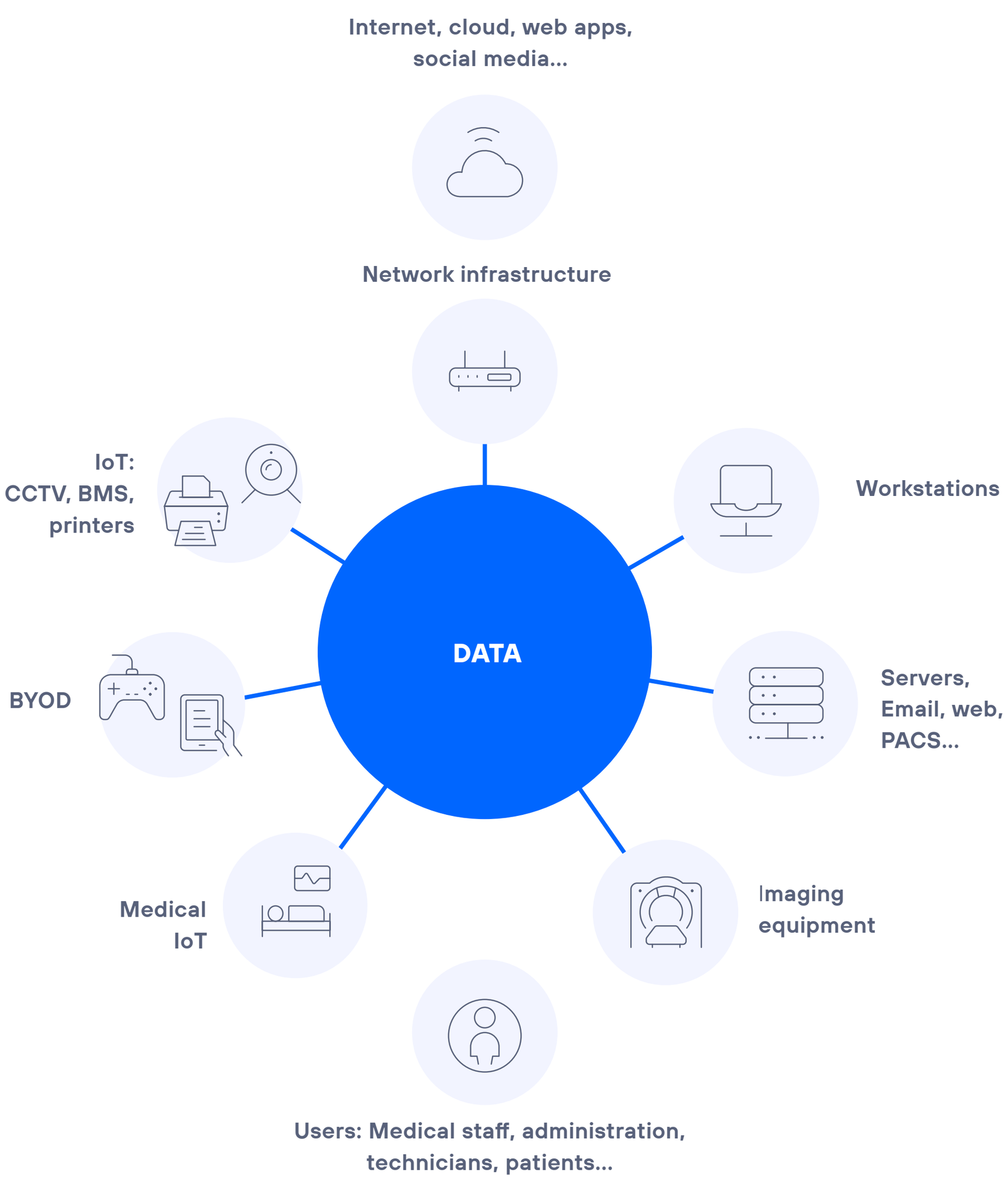
Lives:
Potential loss of life due to the collapse of digital services that support healthcare in situations requiring inmediate action.

2 Cyber Security for Healthcare

2.1. The environment

The first step in the cyclical path of cyber security is to understand the environment that is to be defended. In the case of the healthcare environment, there are several particularities that characterise it, such as the large number of different users with access to services, devices and information, the criticality of the confidentiality of the data handled, the direct impact that a cyber-attack can have on the health and well-being of users, and the great public repercussions it has in the press, among others.

The following diagram represents a high-level overview of a healthcare environment, with various types of assets, users and data as its main focus:



2.2. Security weaknesses

In terms of cyber security, the healthcare environment is at high risk of cyber-attacks as it is the convergence of a myriad of heterogeneous elements: classic IT systems, medical devices, personal devices and IoT, among others. The vulnerability of hospitals is even higher due to the number of people with the potential to physically access hospital assets, which can lead to cyber security breaches. Security weaknesses are defined by four pillars of focus:

Government: The lack or ineffectiveness of a cyber security governance model established by the organisation's management is the first difficulty in improving security. Without well-defined roles, assigned responsibilities, a set of policies and procedures, and a plan to follow, it is impossible to make a return on the efforts and investments made in this area.

Identity: In an environment characterised by a large number and variety of users and applications, the absence of identity controls to ensure, firstly, the identity of individuals and, secondly, the principle of minimum privilege, that is, that each person can access only the minimum required, increases the attack surface. This has a major impact in the context of home working and remote access to the hospital network.

Net: The network that connects all systems and through which all data flows in a hospital is critical. Reliable access control is necessary and capable of dealing with the heterogeneous coexisting systems. It is common to find hospital infrastructures without such control and, moreover, with sub-networks that are not properly segmented and connected to systems that are unknown in purpose and functionality.

Devices: Devices are one of the weakest assets in the healthcare environment. Common security issues include: the use of legacy and/or outdated applications and operating systems, long lifetimes and lack of hardening processes that make such upgrades difficult, and security misconfigurations in applications and protocols. IoT devices are a particularly problematic case as they cannot be managed or controlled in detail and can be modified by people with physical access.

The weaknesses presented can be exploited by cyber criminals, both from outside and inside the perimeter that comprises the hospital infrastructure. The most frequent cyber-attacks in healthcare:

- **Ransomware:** This attack involves infecting a computer with malware that encrypts its hard drive and demands a payment to return the contents to the user. It is one of the most common and profitable attacks for cybercriminals as many organisations agree to the extortion even though they have no guarantee of getting their files back.

- **Data theft:** Another of the most profitable attacks for cyber attackers is data theft, as clinical data is particularly prized on the black market, in fact, there are also cases of attempted theft of research files and evidence.

- **Denial of service:** A denial of service can be the result of a ransomware attack that renders computers useless, but it can also be an end in itself that seeks to damage the service provided. It is particularly damaging in the case of healthcare as the saturation of systems and services in a hospital puts at risk human lives that depend on their proper functioning.

2.3. ENISA security recommendations

There are several sets of recommendations for improving security in healthcare environments created by organisations such as NIST and ENISA. These suggestions include organisational and technological aspects, which are listed below:

Organisational measures

Establish a cyber security governance plan:
Establish roles and responsibilities in the organisation for cyber security and create a set of policies and procedures for cyber security use.

Risk management:
Risk identification and analysis are the first steps in understanding the current situation and prioritising the controls and countermeasures to be deployed. The completion of all phases of risk management will be crucial to maintain a manageable level of risk.

Staff awareness and training:
Raise awareness among all hospital staff with access to IT systems about cyber security risks and what they can do to protect themselves from cyber criminals.

Implement a contingency and continuity plan:
It is necessary to be prepared and have a contingency plan indicating what to do in the event of a cyber-attack to maintain operations and return to a state of normality.

Conduct regular security audits:
A security audit helps to identify new points of failure and to consolidate improvements to previously implemented controls. While the pace of technological evolution means that auditing must be repeated periodically, today's technology solutions help mitigate the time and cost requirements of regular auditing.

Technical measures

Implementing network monitoring and intrusion detection:
Monitoring can detect attacks and anomalies in the network, such as the lateral movement of an attacker or an infected IoT device used as a command and control node.

Making and keeping backup copies:
Keeping important information backed up is an essential measure to protect against accidental failures, human error and attacks such as ransomware.

Apply network access control:
In an environment with a wide variety of users and devices, it is essential to control who accesses the network and to apply the necessary policies depending on the type of user or device.

Apply network segmentation policies:
Adequate segmentation limits the propagation of attacks, allowing only the minimum necessary communications.

Automatic asset discovery and inventory:
A crucial part of security in IoT environments is an automatic and detailed inventory of unmanageable devices to actively manage their risks.

Apply data encryption where necessary:
Encrypting data at rest and in transit with a robust procedure greatly reduces the risks of unauthorised use. Secure data deletion is also advisable in specific contexts.

Running anti-malware software on endpoints:
Endpoint protection software prevents many problems such as malware infections and exploitation
of vulnerabilities in devices that support it.

Apply patching, upgrading and configuration procedures:
A good patching and configuration policy is key to security, but in many cases it is not possible to patch devices, so the use of virtual patching is recommended to protect them from current and future vulnerabilities.

Authentication and authorisation mechanisms:
Establishing identification and authorisation mechanisms is essential to maintain control over which users can access which content and services, thereby limiting the impact if an account is compromised.

3 Telefónica Tech's proposal for Healthcare

In Telefónica Tech we have been helping our clients in healthcare to face and manage cyber security risks since the beginning of the digitalisation of this sector. In this context, we have created a special proposal, with a comprehensive approach to cyber security based on 3 main pillars: **processes, technologies and management.**

3.1. Processes

Cyber securimty is not a goal to be achieved but a continuous and periodic process of review and improvement. This cyclical process can be summarised in 3 phases, and we at Telefónica Tech can help you:

- **Security audits:** A security audit provides information on the current status, level of compliance, weaknesses and effectiveness of the measures that have previously been implemented. Telefónica Tech can carry out these audits both in general security audits and audits against a standard such as ISO27000, including ethical hacking exercises.

- **Development of the cyber security Master Plan:** Once the current status is known through an audit, it is time to draw up a Master Plan that defines the improvement actions to be taken in that iteration of the cycle. Telefónica Tech has a large team of experts who can help draw up a complete, ambitious and realistic Master Plan to carry out the following steps.

- **Implementing measures:** The last phase is to carry out the actions that have been proposed in the previous point, however, although it sounds simple, the implementation of the measures is one of the most complicated points of the process. Telefónica Tech provides the experience of its experts to deploy the technologies and changes determined in the plan.

3.2. Technologies

There are several sets of recommendations for improving the security of healthcare environments created by organisations such as NIST and ENISA. These suggestions include organisational and technological aspects, which are listed below:

Segmentation: Adequate separation between network segments is a key measure to hinder lateral movement and limit potential malware infections.

Virtual patching: When it is not possible to keep an asset patched, virtual patching can be used to mitigate the risk of an attacker exploiting its vulnerabilities.

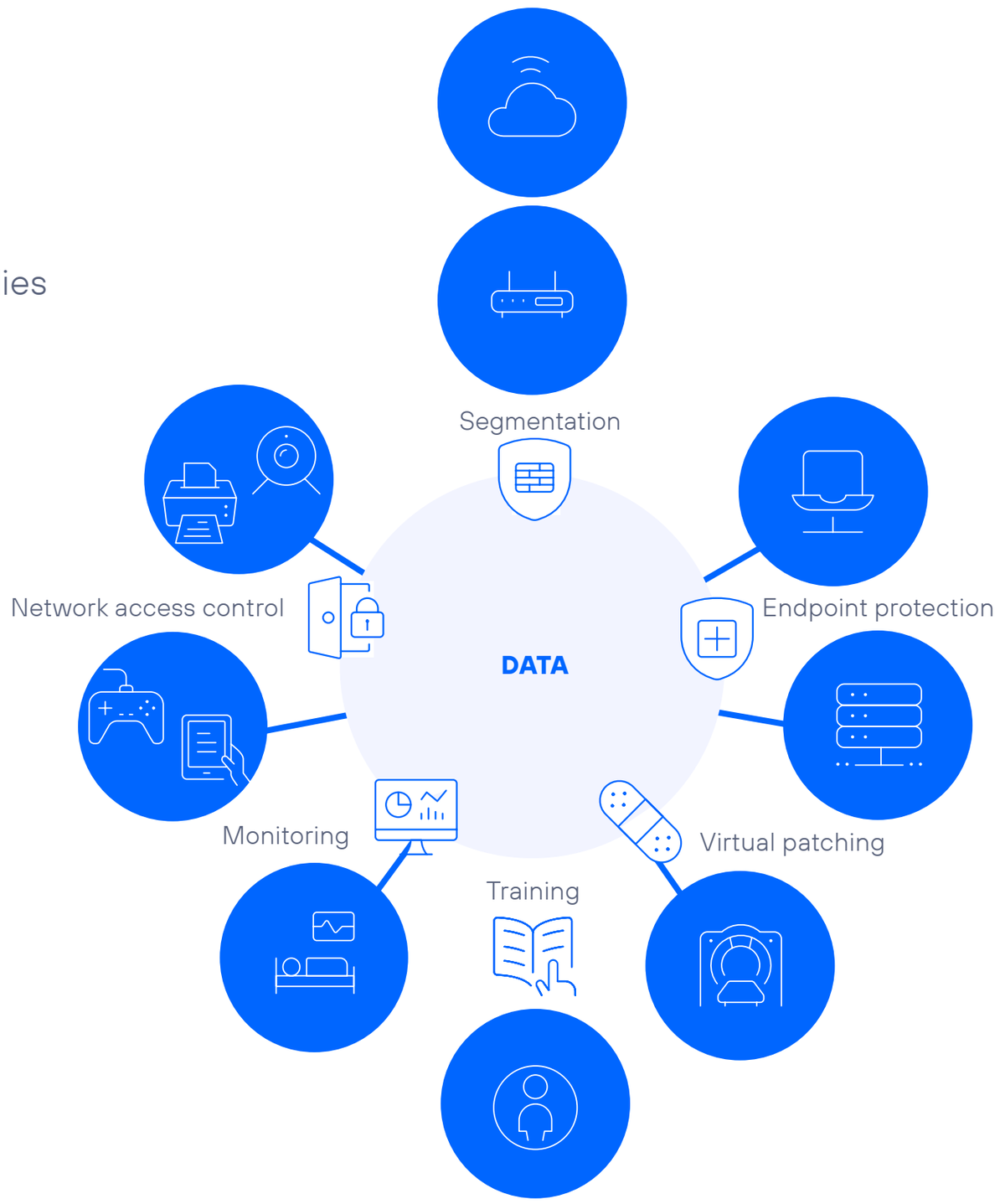
Network access control: The deployment of a Zero Trust architecture enables fine control of devices, users and applications so that everyone can perform the functions they are authorised to do, when and how they are authorised, as well as being able to monitor malicious activity and have activity logs in case they need to be audited.

Security monitoring: A monitoring service deployed in the hospital network offers many benefits. The first is an automatic inventory of devices, especially IoT-M, by interpreting their native protocols such as Dicom and HL7. The second is the complete visibility of device behaviour, being able to detect attacks, anomalies and even errors.

Endpoint protection: An endpoint protection software that supports it can prevent a large number of threats to users such as fraudulent websites, infected files, and exploitable software, among others.

Training and awareness: People are the weakest link in the cyber security chain, so it is crucial that employees are made aware of the risks involved and how to avoid them.

Others: Telefónica Tech offers many other technologies with useful functionalities for the hospital environment, such as secure remote access, data deletion or honeypot-based attacker deception.



3.3. Management

Although the technologies and measures have already been deployed, they will not be effective without a good management and improvement process. Telefónica Tech has a global SOC distributed in various locations around the world from which it provides services such as:

- **24/7 security monitoring:**
  Monitor the alerts generated by security tools on a regular basis to ensure a quick and effective response in the event of a problem.

- **Regular security status reports:**
  Sending bespoke reports on a regular basis helps the organisation to keep up to date on its security, taking into account any new developments or changing trends.

- **Expert incident response**:
  In the event of a security incident, Telefónica Tech's SOC experts are committed to investigating and resolving the incident.

- **Security technology maintenance and optimisation:**
  Technologies can also be maintained and optimised from the SOC, improving their capabilities, adding new functions and keeping them up to date and always ready.

About Telefónica Tech

Telefónica Tech is a key holding of the Telefónica Group. The company offers a wide range of integrated technology services and solutions in Cyber Security, Cloud, IoT, Big Data and Blockchain. Telefónica Tech's capabilities reach more than 300,000 customers in 175 countries every day.

More information

telefonicatech.com

Telefónica Tech