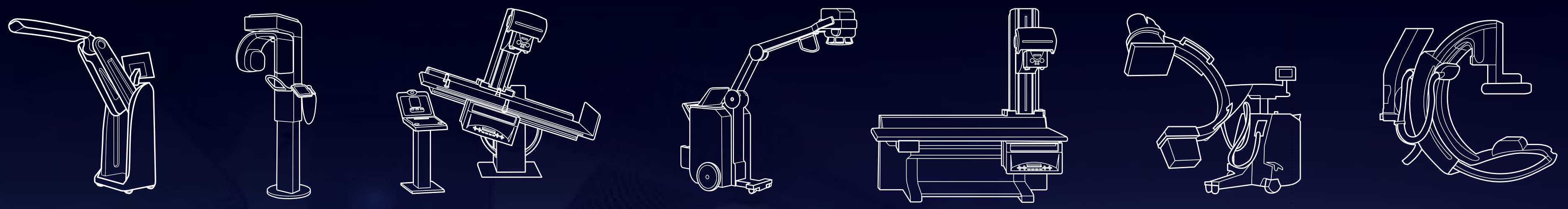
thalesgroup.com

THALES
Building a future we can all trust

Thales's end-to-end comprehensive offer for **Connected Radiology**



Thales’s end-to-end comprehensive offer for **Connected Radiology**

As in many sectors, the COVID crisis has substantially changed the way of working, with an increasing need for digital solutions to guaranty continuity of services. The same applies for the medical domain.

During the pandemic, clinicians maintained the link with patients, conducting remote consultations, but raising a huge concern with medical data security flow: Are the communications secure enough? Are the patient’s data stored securely? Is the data access management well identified?

By analogy to the clinical workflow, the continuity of services of medical equipment is also critical. Pandemic working conditions highlighted the need for remote solutions to guaranty the medical technical workflow. Thales’s dedicated medical connectivity solutions and advanced security expertise allow medical device manufacturers to meet the security and connectivity requirements for remote maintenance. Original Equipment Manufacturers (OEMs) need to inspire confidence and trust in their maintenance services for clinical, financial and organizational work flows. At Thales, we deeply believe that our expertise and solutions can help fulfill that purpose. Our value proposition for OEMs revolves around four key features we believe every remote maintenance service must deliver:

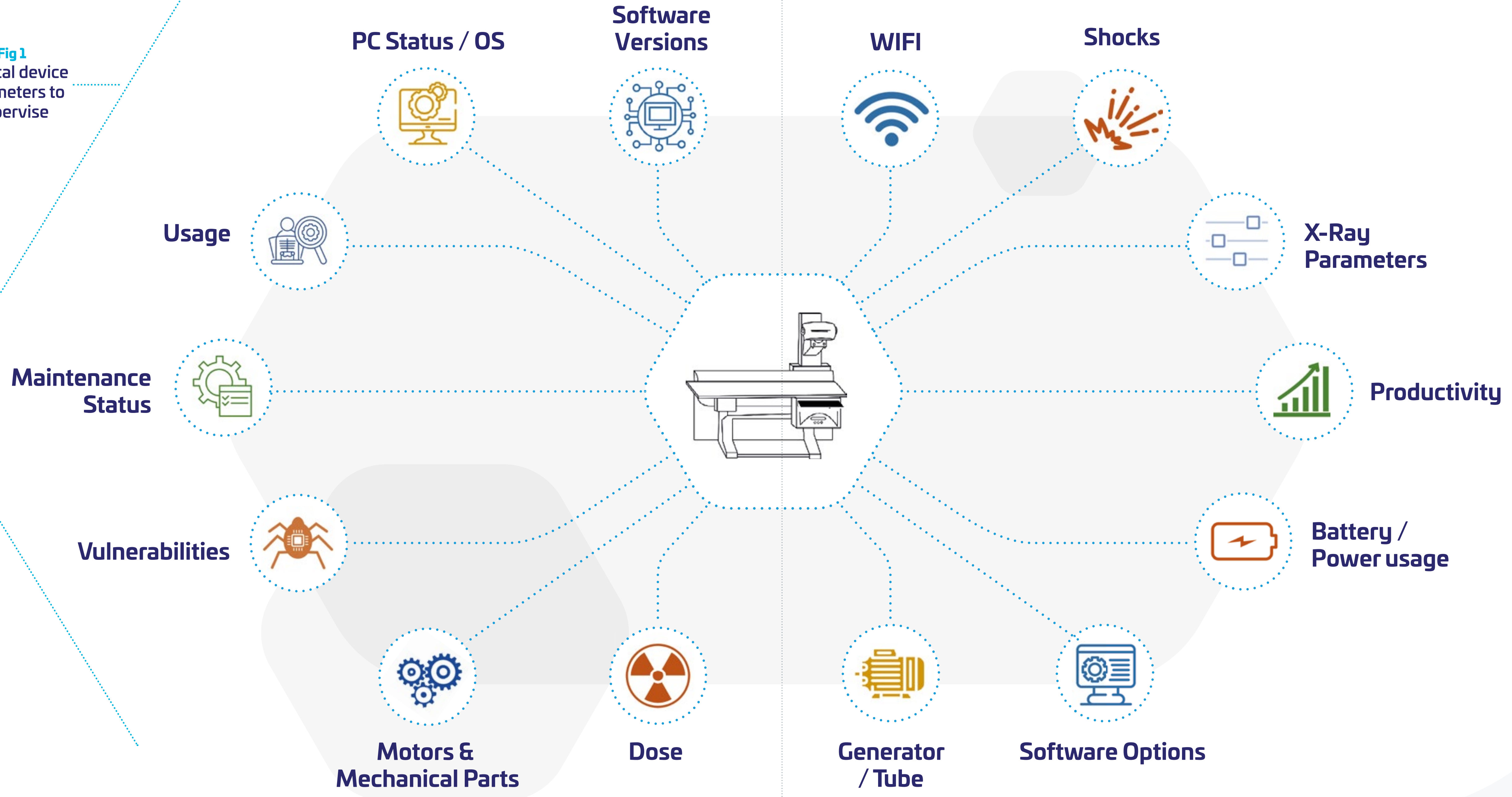
- **Robust and trusted security**
- **Always-on, reliable connectivity**
- **Security and Integrity of data storage**
- **Worldwide and seamless operation**

We have developed solutions that incorporate these four principles and combine high-end connectivity with robust cybersecurity to meet the requirements of medical manufacturers.

Remote device maintenance

The results of a survey published in an article from Lorna Young, IMV, in auntminnie.com, underpin the need for remote maintenance. When asked to indicate which types of support will be more important to have in future service contracts, imaging departments are likely to seek value-added in remote and software-related services in addition to the classic "break-and-fix" services, including "remote diagnostics", "cybersecurity services", "remote repair of software", "software upgrades for new clinical capabilities", and "software updates for bug fixes". Interestingly, these value-added services will work well, as the "new normal" may require even more sophisticated virtual solutions. [1]

Fig 1
Medical device parameters to supervise



New threats coming with connectivity

Nevertheless, adopting digital technologies increases what cybersecurity experts call the “surface attack”, meaning protection of the IT systems is not sufficient any more, as all connected devices (Personal computers, mobile phones, wearables, medical equipment,…), data communications, cloud environments with access to the IT/OT systems of the hospitals must also be protected at the required level of security. Otherwise, they are potentially weak areas that cyber attackers can exploit, penetrate through, and reach the whole hospital IT systems. It is like a castle with thousands of doors and windows. Attackers want to find that single unlocked door or window.

In the last 5 years, under protected and highly critical hospitals have been targets for cyber criminals. In France, hospital attacks have increased by 37% between 2020 and 2021 (source French Security Agency ANSSI [(2)]), meaning three cyber intrusions per day!

In the US, The FDA [(3)] has announced that cybersecurity threats to the healthcare sector have become more frequent and more severe. Indeed, cybersecurity attacks may take control of medical devices and interrupt hospital services, with dramatic consequences.

Motivations from attackers can be financial (ransomware), or other such as geopolitical or terrorism. Ransomware attacks on healthcare organizations were predicted to quadruple between 2017 and 2020 [(4)], and are expected to be weaponized by 2025 (Gartner Press Release, July2, 2021 [(5)])

Between 2020 and 2021, France recorded 27 major cyberattacks in healthcare institutions. Last year, February was the most impactful month for attacks on hospitals.[(4)]

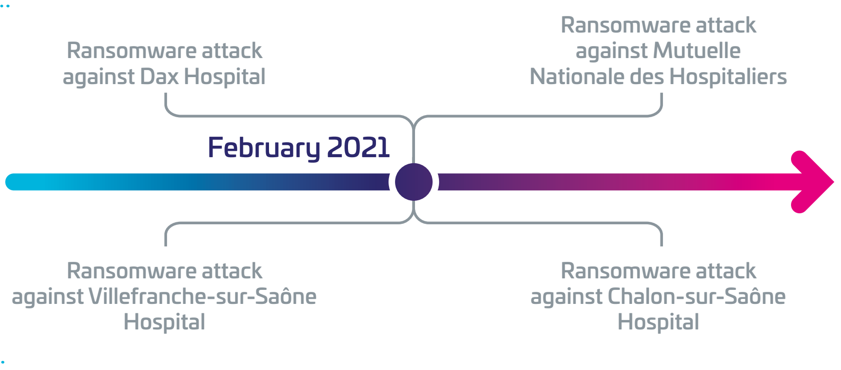
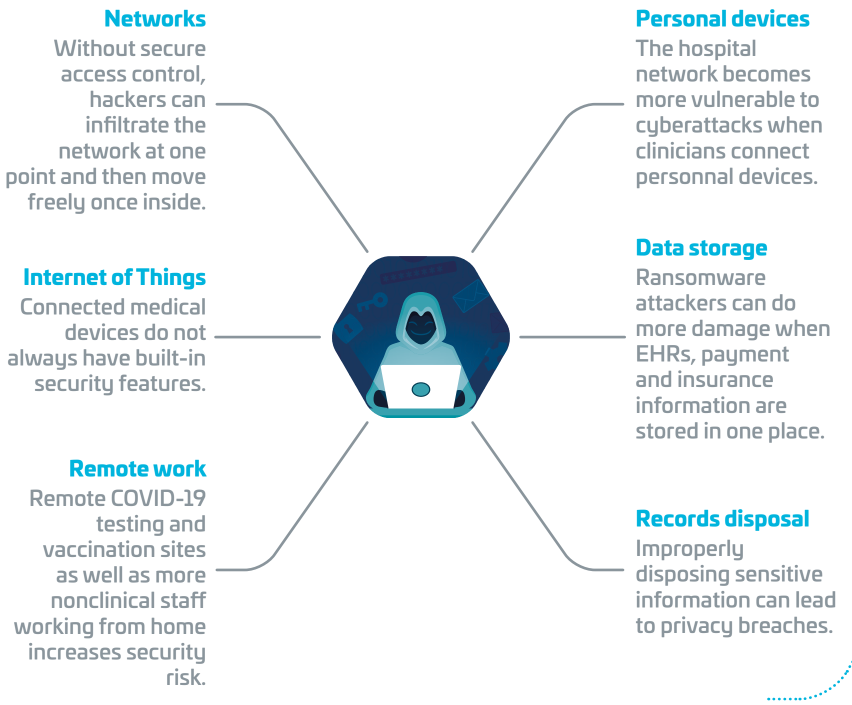

Ransomware attack against Dax Hospital
Ransomware attack against Mutuelle Nationale des Hospitaliers
February 2021
Ransomware attack against Villefranche-sur-Saône Hospital
Ransomware attack against Chalon-sur-Saône Hospital

Fig 2
Cyberattacks on French health care facilities in february 2021 [(4)]

In the US, Universal Health Service (UHS), with 3.5 million patients, and 400 facilities in the US and UK, faced the Ryuk ransomware, reporting a loss of around $67million [(4)]. Cyber attackers are more and more organized, developing sophisticated attacks, which are difficult to detect. In 2020, the estimated global impact from ransomware reached $350 million [(6)]. More than 93 percent of healthcare organizations have experienced a data breach over the past three years, and 57 percent have had more than five data breaches during the same period. [(4)]



Networks
Without secure access control, hackers can infiltrate the network at one point and then move freely once inside.

Internet of Things
Connected medical devices do not always have built-in security features.

Remote work
Remote COVID-19 testing and vaccination sites as well as more nonclinical staff working from home increases security risk.

Personal devices
The hospital network becomes more vulnerable to cyberattacks when clinicians connect personnal devices.

Data storage
Ransomware attackers can do more damage when EHRs, payment and insurance information are stored in one place.

Records disposal
Improperly disposing sensitive information can lead to privacy breaches.

Fig 3
Six vulnerabilities points hackers target in hospital cyber attacks [(4)]

At HIMSS 2021, Keren Elazari, famous Cybersecurity Analyst, mentioned at a keynote that “it is not a question of how or if, but when”. Intrusions will happen and hospitals should be ready for it, with adapted protection and governance, trained cyber analysis team, communication plans, etc. [(7)]

In the Thales annual Data threat report 2022 [(8)], it was pointed out that “While there is a positive trend in use, encryption levels are still below what is needed for comprehensive protection.” Healthcare respondents declared that they manage with encryption at 61% and reported key management at 55%.

There is still a significant disconnect between interest and action.

Need to comply with new regulation

Regulatory institutions need to adapt their requirements and their standards. Very recently, the FDA published a preliminary document, stating that: Increased connectivity has resulted in individual devices operating as single elements of larger medical device systems transforming medical devices from black closed boxes to "open" ones. These systems include health care networks, medical connected devices, and medical applications, to give just a few examples. Consequently, without adequate cybersecurity considerations a cybersecurity threat can compromise the safety and/or effectiveness of a device by compromising the functionality of any asset in the system. [3]

The US National Institute of Standard and Technology (NIST), has specified a cybersecurity framework that gives a methodology to build on a long term cybersecurity resiliency for high sensitive operational systems [9]. This framework is commonly used by security industries and adapted according to the risk of cyber threat, and level of protection needed.

Regarding Europe, Medical Device Regulation (MDR) is claiming that: safety, security and effectiveness are critical aspects in the design of security mechanisms for medical devices. Therefore, there is a clear requirement that safety and security needs to be considered by the manufacturers from the very early stage of conception and design, to development and manufacturing process and throughout the entire life cycle. [10]

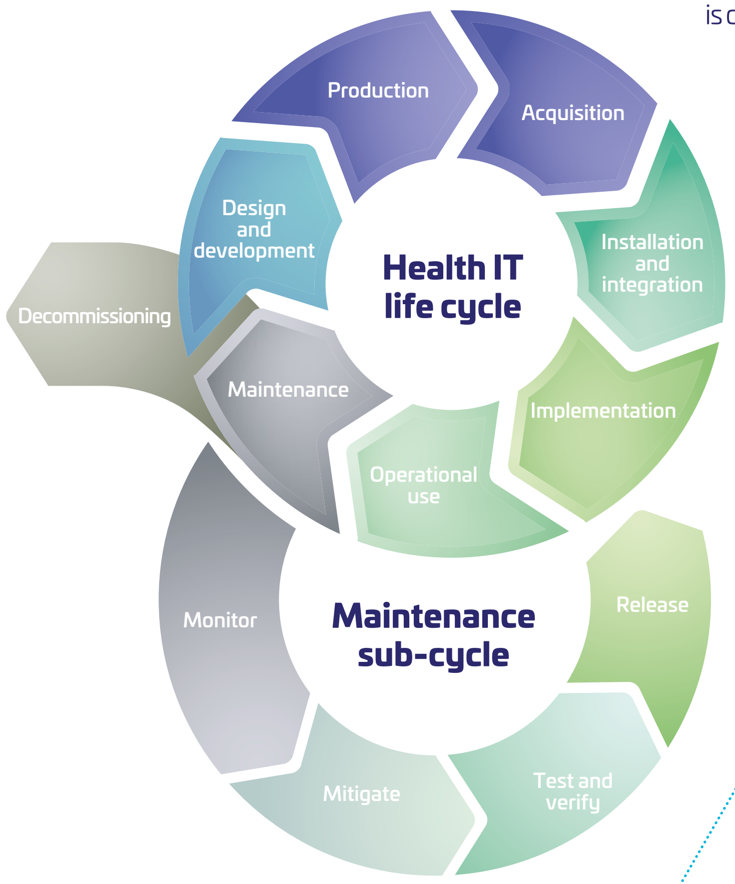


Fig 4
Life cycle stages [10]

As a consequence, the OEMs need to take into consideration more and more the product lifecycle and its evolving environment in their daily usage, beyond the "manufacturing" process. As part of the hospital network, OEMs need to interact with the network environment of their customers. This is far from being an easy task when the scope of the medical device is supposed to be clearly defined and "frozen". Somehow, it means that medical systems become "dynamic" and need to be perpetually re-evaluated, updated tested, distributed, documented. (cf. figure above)

Indeed, in the MDR guidelines [10] it is mentioned that:

During the support lifetime of the device, the manufacturer should put in place a process to gather information with respect to the security of the device. This process should take into account:

1. Security incidents directly related to medical device software.
2. Security Vulnerabilities that are related to the medical device hardware/software and the 3rd party hardware/software used with the medical device.
3. Changes in the threat landscape, including interoperability aspects.

The manufacturer should evaluate the information thus gathered, evaluate the associated security and safety risk and take appropriate measures that control the risk associated with such security incidents or vulnerabilities.

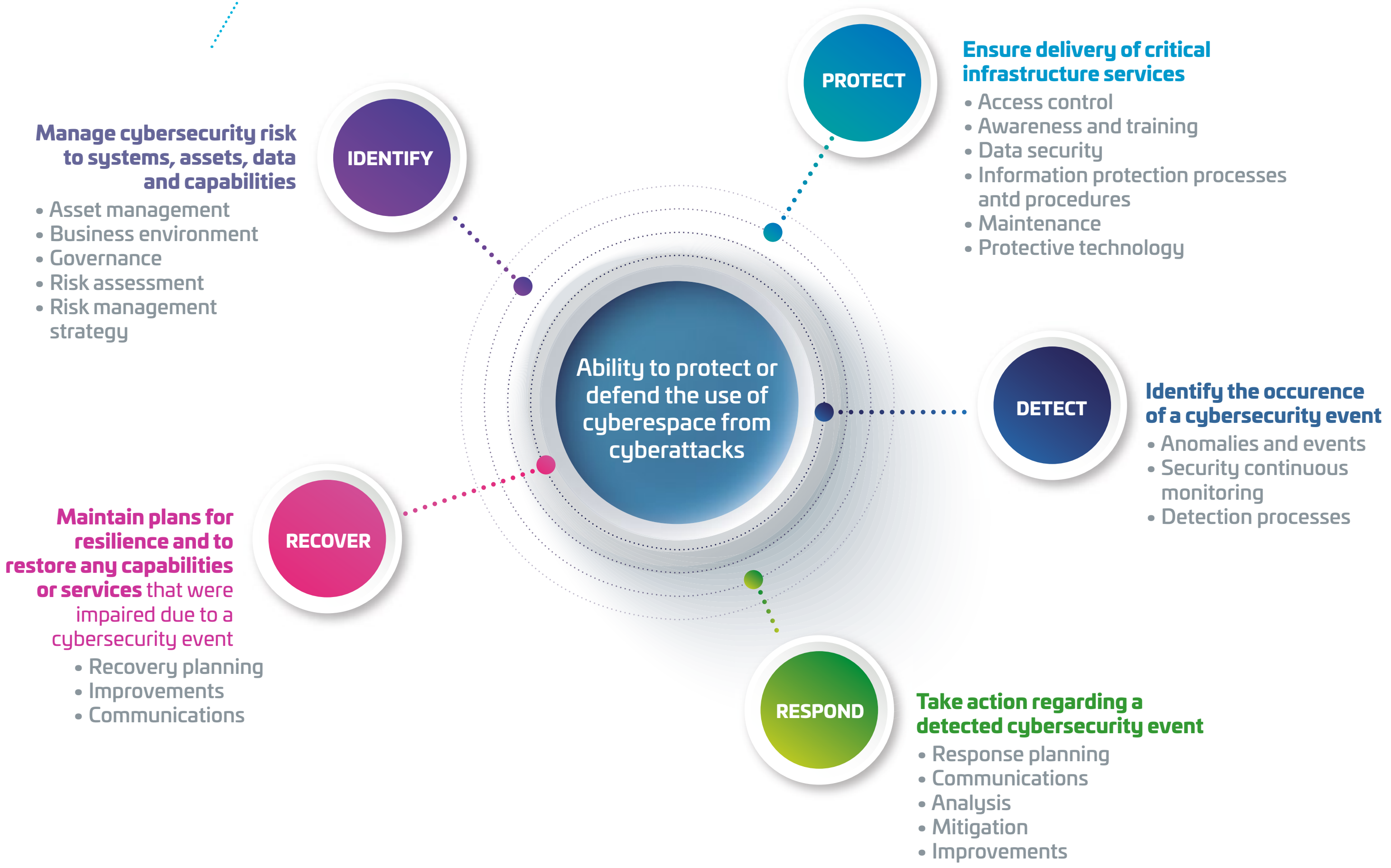
As an example those measures may include:

- Information to operators of medical devices on the identified risk and possible mitigations in the operating environment
- Quick fixes, e.g. network configuration changes.
- Medical device software updates.
- 3rd party software updates or patches.

Leveraging Thales expertise in cybersecurity

To support hospitals and OEMs in their digital transformation, Thales designs, builds and operates cybersecurity solutions and services to protect all critical assets of the medical industry players. We draw on decades of security experience across highly demanding markets from governments to banks where we developed expertise on embedded systems, industrial networks and cloud computing. Our solutions allow the deployment of secure connected services by bringing trust between stakeholders, minimizing risk and protecting end-users' privacy. As mentioned above, NIST framework provides a strategic vision of cyber risk management through five functions: identify, protect, detect, respond and recover. For each of these five functions, Thales offers adapted solutions and services to support its customers and enable them to build their cyber resilience.

Fig 5
NIST Standard Framework


Ability to protect or defend the use of cyberespace from cyberattacks
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

Manage cybersecurity risk to systems, assets, data and capabilities
- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy

Ensure delivery of critical infrastructure services
- Access control
- Awareness and training
- Data security
- Information protection processes antd procedures
- Maintenance
- Protective technology

Identify the occurence of a cybersecurity event
- Anomalies and events
- Security continuous monitoring
- Detection processes

Take action regarding a detected cybersecurity event
- Response planning
- Communications
- Analysis
- Mitigation
- Improvements

Maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event
- Recovery planning
- Improvements
- Communications

Leveraging Thales cybersecurity expertise, we have developed a remote medical device monitor, integrating required levels of protection and security to comply with regulations. It is built to securely collect from radiology systems data, and provide intelligence dashboards for remote maintenance. This enable OEMs to supervise all of their fleet, and anticipates problems in a preventive mode. It reduces equipment downtime, and operational shutdown for the clinical, financial and organizational benefit of hospitals.

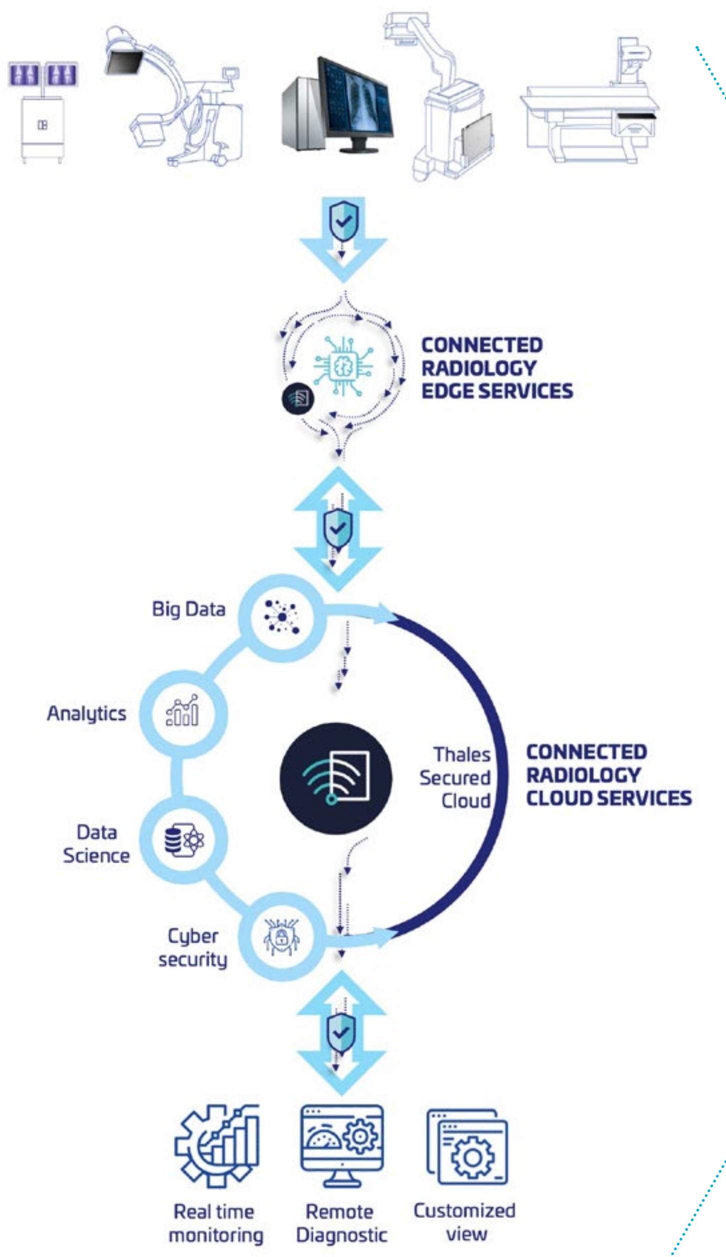


Fig 6
Connected Radiology architecture

Reliable, Secure, Trusted

At Thales we know that connectivity delivers performance, but it must come with reliability and trust.

Our solution is a Cloud solution hosted by Thales and dedicated to monitor radiology systems. Its architecture is built to provide data isolation between customers so that one customer's data will not be shared in any way with other customers.

Connected Radiology provides:

- **Software secured tool** deployed and running on hosts. It collects host metrics, aggregates logs and metrics and shares collected Data with the Cloud part of the Service.
- **Cloud solution**: hosted architecture dedicated to Data storage, processing and presentation.
- **Web administration interface**: permits the management of the Services users and sites.
- **Online Help:** mainly delivers information to create and update dashboards.

Our solution helps OEMS to demonstrate the productivity of their systems, optimize the uptime and bring their customers' satisfaction, while guarantying reliability, security and trust.

To do so, Connected Radiology is built around:

- **Security**: an "end-to-end" service where we control all the components of the data chain: acquisition, transfer, storage and processing. A dedicated Thales cyber analyst team supervising the cloud environment to detect potential threats and respond immediately in case of attacks.
- **Integrity**: all the data are "ID & time stamped" at the acquisition level, to be stored and analyzed in customer specific silos.
- **Trust**: each customer has specific storage requirements with adequate redundancy and level of responsibilities to manage accesses with multi-factor identification.
- **Availability**: our platform guaranties a continuity of service thanks to its infrastructure and monitoring teams.

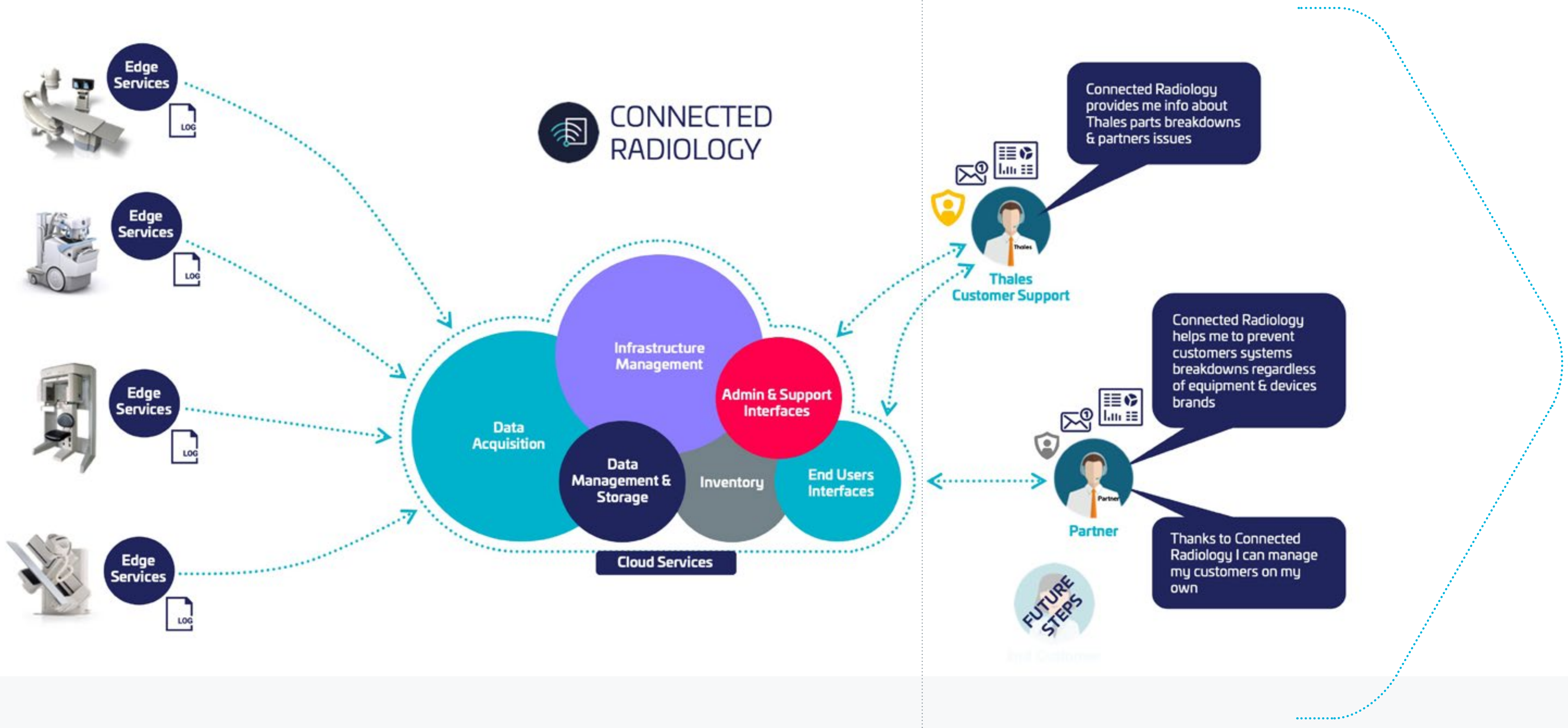

Edge Services
LOG
Edge Services
LOG
Edge Services
LOG
Edge Services
LOG
CONNECTED RADIOLOGY
Infrastructure Management
Admin & Support Interfaces
Data Acquisition
Data Management & Storage
Inventory
End Users Interfaces
Cloud Services
Connected Radiology provides me info about Thales parts breakdowns & partners issues
Thales
Thales Customer Support
Connected Radiology helps me to prevent customers systems breakdowns regardless of equipment & devices brands
Partner
Partner
Thanks to Connected Radiology I can manage my customers on my own
FUTURE STEPS
End Customer

Fig 7
Connected Radiology principles

Conclusion

Our healthcare ecosystem becomes digital for the benefit of the patients, and the practitioners. But it must come with security. At Thales, we have a DNA of innovation whilst investing heavily in the four key digital technologies of Connectivity, Big Data, Artificial Intelligence and Cybersecurity. Leveraging our solid technological foundations, we support medical system manufacturers in all aspects of remote medical device maintenance. From the medical parameters to controlling the entire life cycle of systems, we guarantee the security, trust and reliability of installed equipment for safer hospitals.

Bibliography

(1) IMV: COVID-19 changes service needs for imaging equipment By Lorna Young, *AuntMinnie.com* contributing writer

(2) Communiqué de presse ANSI du 9/03/2022

(3) Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions - Draft Guidance for Industry and Food and Drug Administration Staff

(4) The cybersecurity handbook 2022 – Thales *http://cyberthreat.thalesgroup.com/*

(5) Gartner Press Release, July 2, 2021

(6) Le-Monde _ Comment fonctionnent les cyberattaques aux rançongiciels qui ont ciblé des hôpitaux- 17 février 2021.

(7) HIMSS21 Keynote: Healthcare Cybersecurity Resilience in the Face of Adversity | Healthcare Innovation (*hcinnovationgroup.com*)

(8) 2022 - Thales Data Threat Report

(9) *Cybersecurity | NIST*

(10) MDCG 2019-16 Guidance on Cybersecurity for medical devices

THALES
Building a future we can all trust

2 rue Marcel Dassault
78141 Vélizy Villacoublay Cedex – France

For further information, please contact:
MIS.sales-contact@thalesgroup.com

> thalesgroup.com <

temps présent - www.tpcommunication.com - © Thales -06-2022
This leaflet cannot be considered as a contractual specification - Photos credits: © Thales