PHILIPS

Azurion

Cybersecurity

Cybersecurity woven into every layer of your interventional suite

Philips uses secure by design and defense in-depth approaches to secure your interventional suite. This paper walks you through those approaches, and the solutions that make up multi-layered systems way of working to protecting data confidentiality and system integrity.

The challenge

Advances in image-guided therapy demand an equally sophisticated cybersecurity strategy

It may be surprising that for all its benefit, the revolution in connected health devices is still in its infancy. Ever- more sophisticated devices and solutions are achieving higher order goals of user friendliness for clinicians and assisting staff. Breakthroughs that enhance clinical outcome are now embedded in procedure efficiency with smoother workflows bring relevant data directly into clinicians' view.

This white paper looks at how the far-reaching benefits of connected imaging devices translate into an evolved strategy for cybersecurity. We walk you through that strategy and detail the technologies that keep your Azurion system cybersafe (see box on Azurion).

Increasing sophistication means that hackers have more ways to enter your system while incentives for them to do so are increasing all the time. Recent studies suggest that confidential patient data is 50 times more valuable on the black market than financial data.[1] This means that your goal of providing excellent levels of care provides criminals with an opening.

Because our goal is an open, smooth-working interventional lab that serves clinicians and patients, we have created security solutions that serve those outcomes too.

Philips Image Guided Therapy recognizes the importance of securing medical devices and protecting your patient data. Together we can maintain a secure environment by remaining vigilant and identifying the ever-changing cybersecurity threat landscape. We are committed to meeting the needs and requirements of our customers. Our security plans encompass your people, processes, and technology with the goal of ensuring the confidentiality, integrity and availability of critical data - whether at rest or in transit.

*Recent studies suggest that **confidential patient data is 50 times more valuable** on the black market than financial data.*

What is Azurion image guided therapy platform?

Philips Azurion is the next generation image-guided therapy platform that allows you to perform procedures easily and confidently with a unique user experience and integration possibilities, helping you optimize your lab performance and provide superior care.

The mindset

Secure by Design - Philips Secure Development Lifecycle (SDLC)

Industry trends have shown that cyber attacks are moving to the application layer of products and pose a significant threat to customers and patient information over the Internet of Things (IoT). According to data collected by the Internet Storm Center, over 70% of attacks on networks are against the application layer.

We strenghten the resilience of our products and services by applying capabilities, components, and techniques, including practices that align to ISO standards (see box), a practical and well-tested means of incorporating security and privacy within the software development process.

Leveraging this methodology, requirements and controls are addressed at each phase of the secure development lifecycle, including the use of Product Security Risk Assessment (PSRA), Data Protection Impact Assessment (DPIA) processes, static code analysis, third party Software Bill of Materials (SBOM) analysis, ethical penetration testing, and continuous product security training across the Philips organization. While tools and processes are key to the Philips SDLC, Secure by Design is a mindset that requires an end-to-end approach beginning with architecture and high-level design which progresses through to coding, testing, and post-market support.

For the interventional suite in particular, these cover twenty different areas including: authorization, audit controls, emergency access, data integrity and authenticity, storage confidentiality (encryption 'at rest'), and transmission confidentiality/integrity (encryption 'in transit'). They map to recognized security frameworks and standards from around the world.

Security standards Including but not limited to:

IEC 80001

ISO 27001

ISO 27034

ISO 27002

ISO 27018

NIST SP 800-53

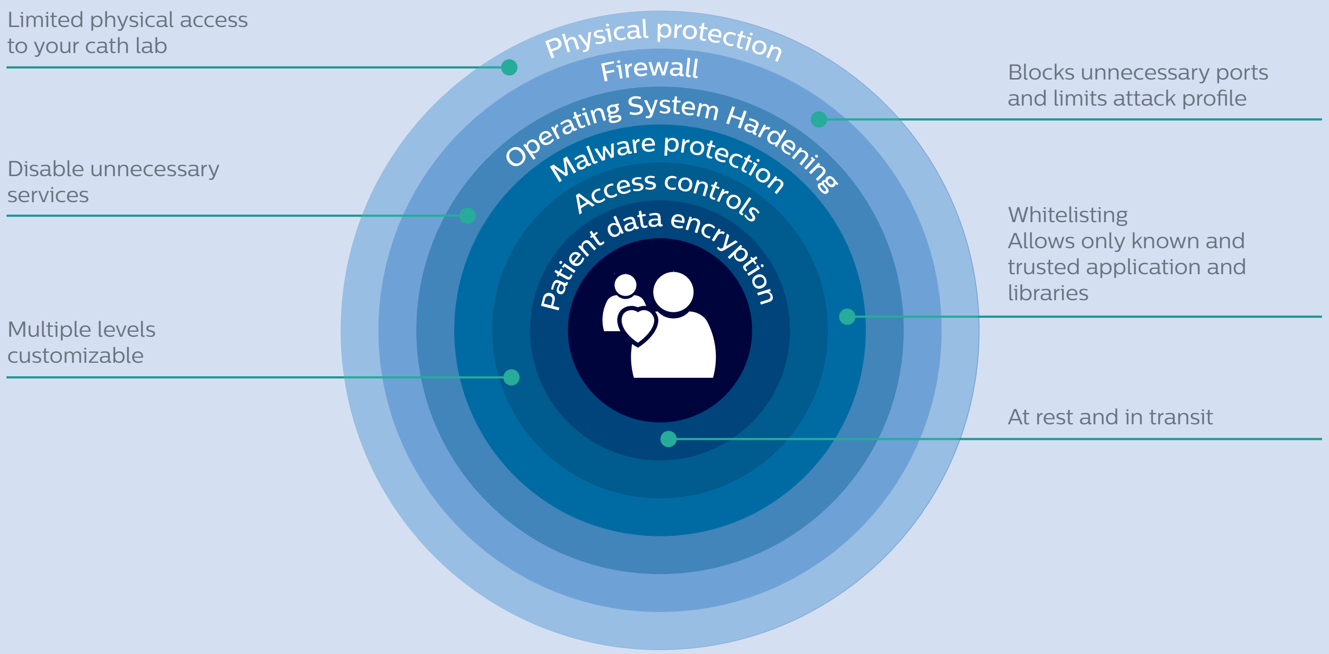
The strategy

Defense-in-depth

Your hospital will be well acquainted with the Swiss Cheese model of patient safety, whereby cumulative acts prevent threats to the life of the patient. Defense-in-depth is precisely the same strategy: even if one layer fails several others will counter the attack. This has the result of countering attacks that may arise through diverse vectors.

The diagram below shows how a multi-layered defense is more difficult to penetrate than a single barrier, and is the basis for best practices in medical device security. The layers can include security policies, procedures, access controls, technical measures, training, and risk assessments.

By default, many of these control layers are built in. For others we work with you to optimize your protection of patient data.



Limited physical access to your cath lab
Disable unnecessary services
Multiple levels customizable
Physical protection
Firewall
Operating System Hardening
Malware protection
Access controls
Patient data encryption
Blocks unnecessary ports and limits attack profile
Whitelisting Allows only known and trusted application and libraries
At rest and in transit

Layers in unison

Each layer of the defense in-depth strategy is an effective component in itself. However, their co-operation optimizes your hospital cybersecurity, each layer partnering to limit degrees of risk. They include:

- **Physical protection**
- **Firewall**
- **Operating system hardening**
- **Malware protection**
- **Access controls**
- **Patient data encryption**

Each of these layers plays an important role in helping you thwart hackers, defend against malware, and prevent unauthorized access. We will go through each one and see the distinct role it plays in your interventional suite's cybersecurity.

Physical protection
Attacks are hugely limited by software and hardware measures – this layer makes sure human behavior, hospital process and logistics make your systems watertight from a security point of view. We work with you to look at physical aspects such as lab positioning, staff protocols and general awareness are all in place to enhance security across your interventional suite.

Firewall blocks unnecessary ports
Strict firewall policies limit traffic to and from the Cath lab by blocking all unnecessary ports inhibiting communication with unauthorized computers, limiting the attack profile that a malicious hacker may try to exploit.

Operating system hardening disables unnecessary services
Similar in principle to firewalls, operating system (OS) hardening involves identifying all unnecessary services and functions that are included within the operating system and disabling those not required by the Cath lab systems. OS hardening reduces the attack surface by eliminating those services that may become vulnerable over time. Philips follows the Standard Technical Implementation Guides (STIGs) provided by the Defense Information Systems Agency (DISA).

Operating system patching
What is secure today will not be secure tomorrow. OS patching ensures that latest patches are carefully validated and are made available at a timely, regular frequency. Your interventional suite therefore maintains the latest level of security.

Malware protection via whitelisting provides low maintenance protection
The traditional method of malware protection, anti-virus (AV) software, requires frequent updates to stay current with new viruses and malware being released every day. Hospitals risk being attacked before AV software has addressed new malware.

To mitigate this risk, Philips has implemented the whitelisting solution. Whitelisting protects your Azurion system from malware by allowing only known and trusted applications and libraries to function. Because whitelisting does not need constant updating like traditional AV software, it requires less maintenance and fewer updates.

Access controls can be adapted to your needs
It is estimated that 22% of security breaches since 2020 were due to unauthorized access.[2] To help you control access to data on your imaging systems, with Azurion you can choose from two access control levels:

- Authenticated access: Each user must successfully log in before performing a scan or accessing patient information.
- Direct access: A clinical user may perform exams and access any previously completed exams stored on the system without requiring a login.

With Azurion, you have the ability to create multiple clinical user accounts and multiple hospital administrator accounts. With both systems, hospital administrators have the option of specifying password policies in accordance with local information security requirements and policies.

Patient data encryption at rest and in transit
All patient data stored on the Azurion hard drives is encrypted by default for majority of Azurion systems (depends on local legislation). In addition, you can choose DICOM with TLS for node authentication without encryption, DICOM utilizing TLS encryption, or a combination of the two to encrypt patient data in transit. (This requires corresponding functionality on your PACS system.)

Security Core features

Below is a list of technical features that are implemented in our interventional labs that continue to evolve over time with new releases.

- Firewall policy blocks all unnecessary ports
- OS hardening
  - OS settings utilizing the DISA STIGS
  - Disabled unnecessary services
  - Disable auto-run for removable media
- Media export security
  - Provides the ability to disable export of patient data to removable media
- Malware protection utilizing whitelisting solutions
- Access level
  - No restrictions
  - Only patient data is locked – users may perform exams without requiring a login, but must successfully log in prior to accessing previously completed exams
  - Complete system is locked
  - Users and administrators must successfully log in prior to any system access
- User management policy
  - Local user management
  - Support for unique user accounts
  - Support for unique administrator accounts
  - Management of remote access capabilities
- Password policies – provides the ability to specify password policies for local accounts
- Hard drive encryption – AES-128 and AES-256
- Audit log export – audit logs may be exported utilizing syslog – available protocols are UDP or TLS

Services that keep you Cybersafe

A crucial element of any cybersecurity strategy is ensuring your hardware and operating systems are up to date. We provide hardware and software upgrades through the Technology Maximizer service contract as well as managing one-off OS upgrades. These provide immediate security benefit and can offer ongoing protection through software and hardware upgrade agreements. They have the added advantage of increasing clinical outcomes as well as security for your hospital.

For more information see www.philips.com/technology-maximizer

The commitment

Continuous cybersecurity development

In line with the need to increase security of our products, Philips continues to examine and re-engineer existing products to best accommodate the requirements of our security-minded customers. We are deeply engaged in creating the products of tomorrow based on fundamental security principles.

We will continue to work closely with providers, IT organizations, and customers to provide flexible solutions to today's problems even as we create new Security Designed In products.

For more information, please reach out to:
productsecurity@philips.com

[1] Personal health information is 50 times more valuable on the black market than financial information, according to Cybersecurity Ventures, and stolen patient health records fetch upwards of $50 per record (10 to 20 times more than credit card information). https://www.forbes.com/sites/insights-intelai/2019/02/11/confronting-one-of-healthcares-biggest-challenges-cyber-risk/

[2] 22% of data breaches in 2020 involved the use of stolen credentials. https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

4522 991 63581* OCT 2020

How to reach us
Please visit www.philips.com
healthcare@philips.com