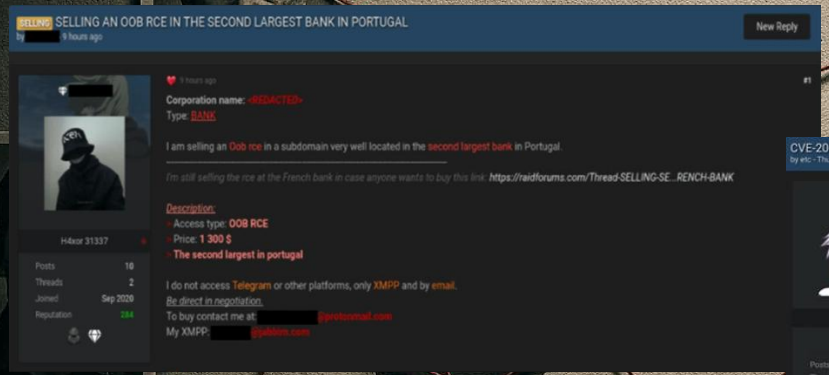
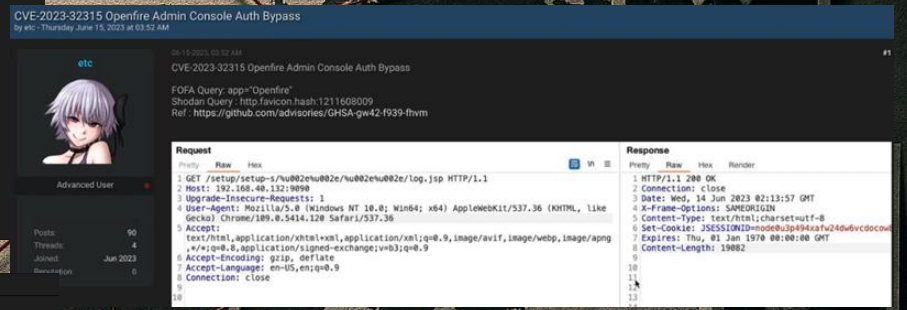


Cybersecurity in healthcare:

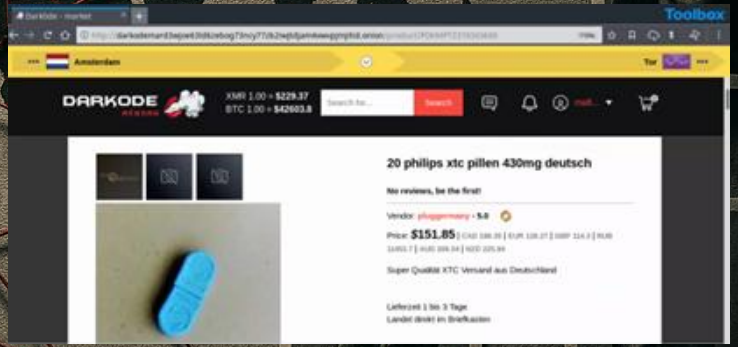
Protecting human lives, not just systems

ORGANIZED CRIME









PHILIPS

Keeping connected care secure

requires the whole ecosystem to work together



PHILIPS

Hospitals require:

Data exchange
Seamless and secure sharing of patient and device data

Artificial intelligence
Access to AI-enabled tools and analytics

Remote expertise
Secure access for remote support and colaboration

Clinical workflows
Integration and clinical applications and systems

SHARED RESPONSIBILITY

- Patient Safety
- Clinical Effectiveness
- Interoperability
- Defense in-depth
- Security by design

Medical device manufacturers are expected to:

Enabling people and patient data to flow
Ensuring seamless, secure data flow across systems, settings and users

Turning data into value
Connecting hardware, software, data and AI to deliver impact at scale

Minimize risk to an acceptable level
Apply risk management throughout the product lifecycle

Meet applicable regulations
Comply with global and local regulatory requirements

Provide transparency and support
Deliver security documentation, updates, and timely advisories



SECURE CONNECTIONS. BETTER OUTCOMES.

- Better patient outcomes
- Efficient clinical workflows
- Strong security posture
- Regulatory compliance

PHILIPS


PHILIPS

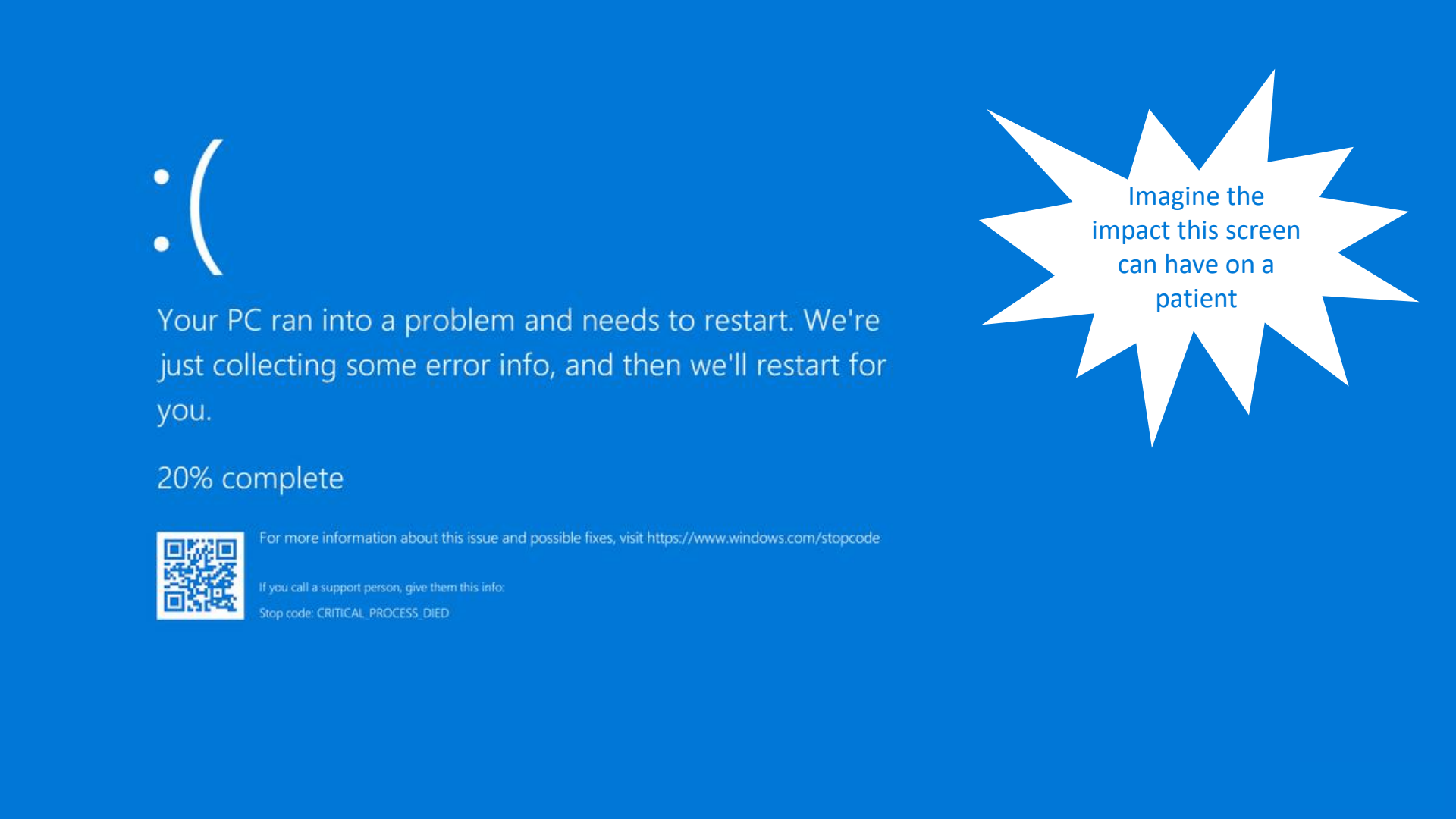


Safety marking plate	Explanation
	Examination room door safety marking plate. The individual symbols are explained in other parts of this section. ext on the safety marking plate: 1. This 1.5T (3.0T) magnet is ALWAYS ON 2. System use and scanning room access for MR Authorized personnel ONLY 3. ONLY screened and approved devices allowed in ing room 4. While scanning: RF fields and acoustic noise

Patient safety safeguarded by mandated use

© Koninklijke Philips N.V.

PHILIPS

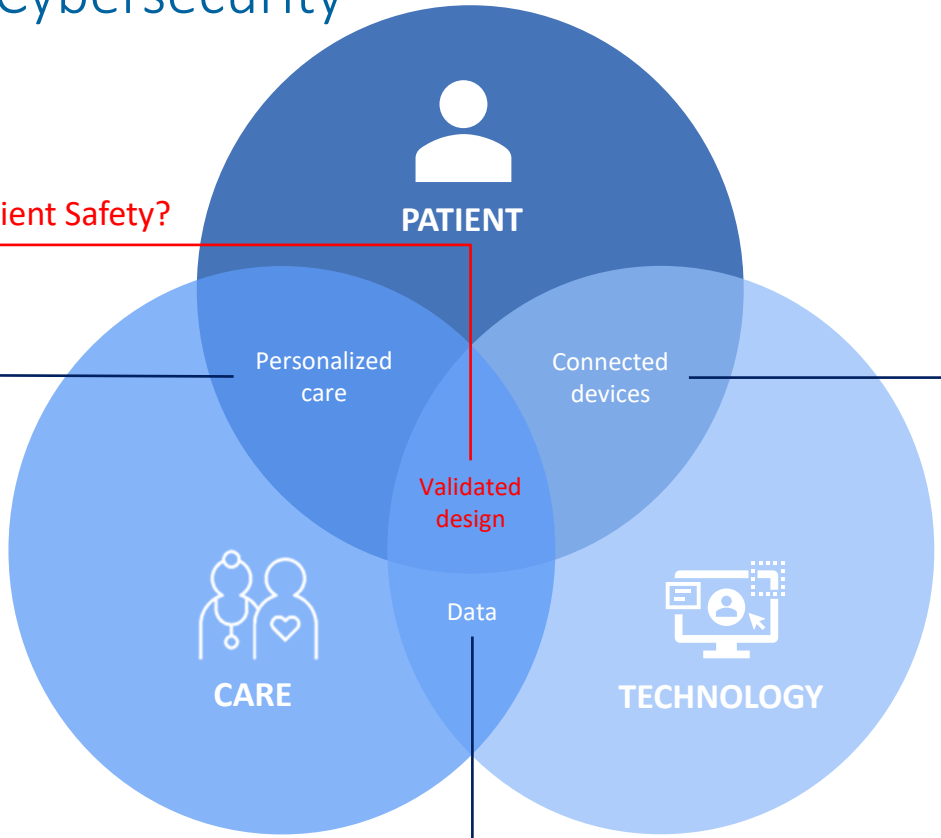

:(
Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.
20% complete
For more information about this issue and possible fixes, visit https://www.windows.com/stopcode
If you call a support person, give them this info:
Stop code: CRITICAL_PROCESS_DIED
Imagine the impact this screen can have on a patient

Medical Device Cybersecurity

Clinical Effectiviness and Patient Safety?

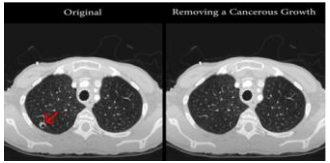
Confidentiality ?







Availability ?



Integrity?

© Koninklijke Philips N.V.

PHILIPS

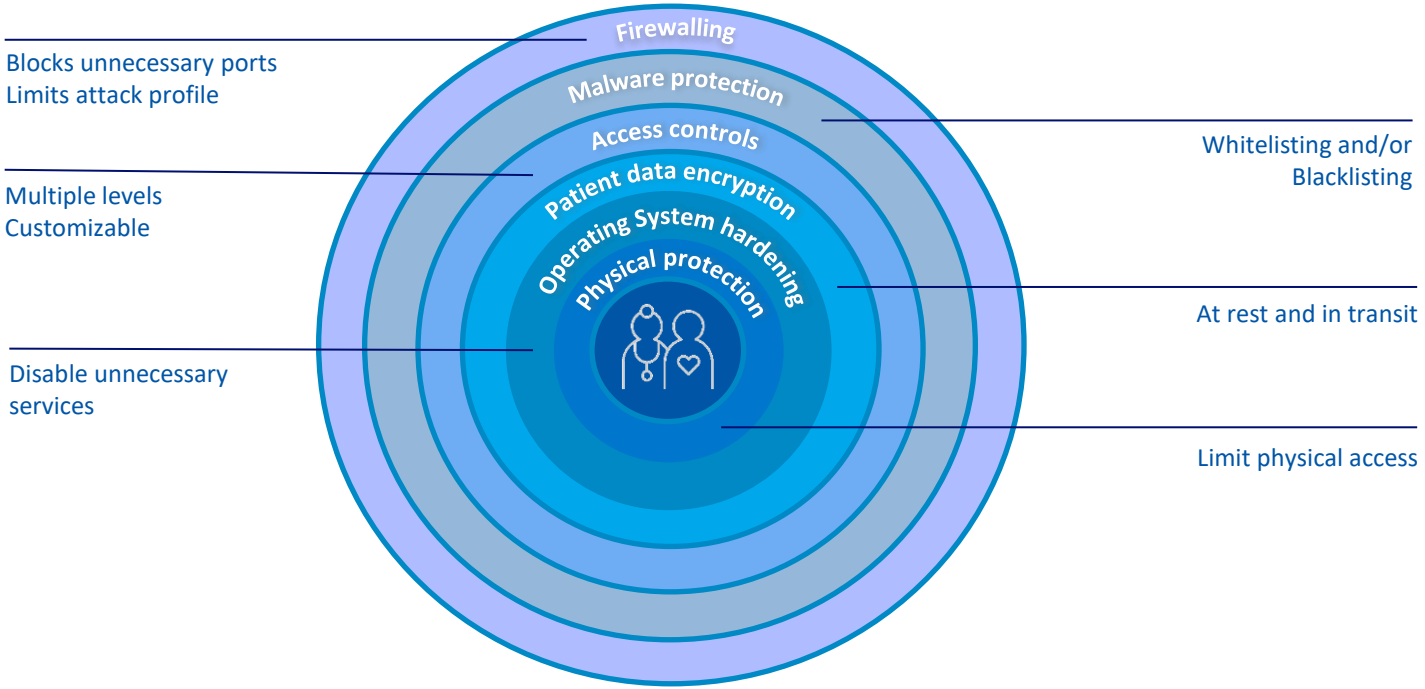
Interoperability enables care, security sustains it



PHILIPS

Philips’ defense in-depth strategy

Defense-in-depth strategy, the idea that a multi-layered defense is more difficult to penetrate than a single barrier, is the basis for best practices in medical device security. With Philips, hospitals and medical practices have the protection to keep health information and medical devices secure, giving patients true peace of mind.

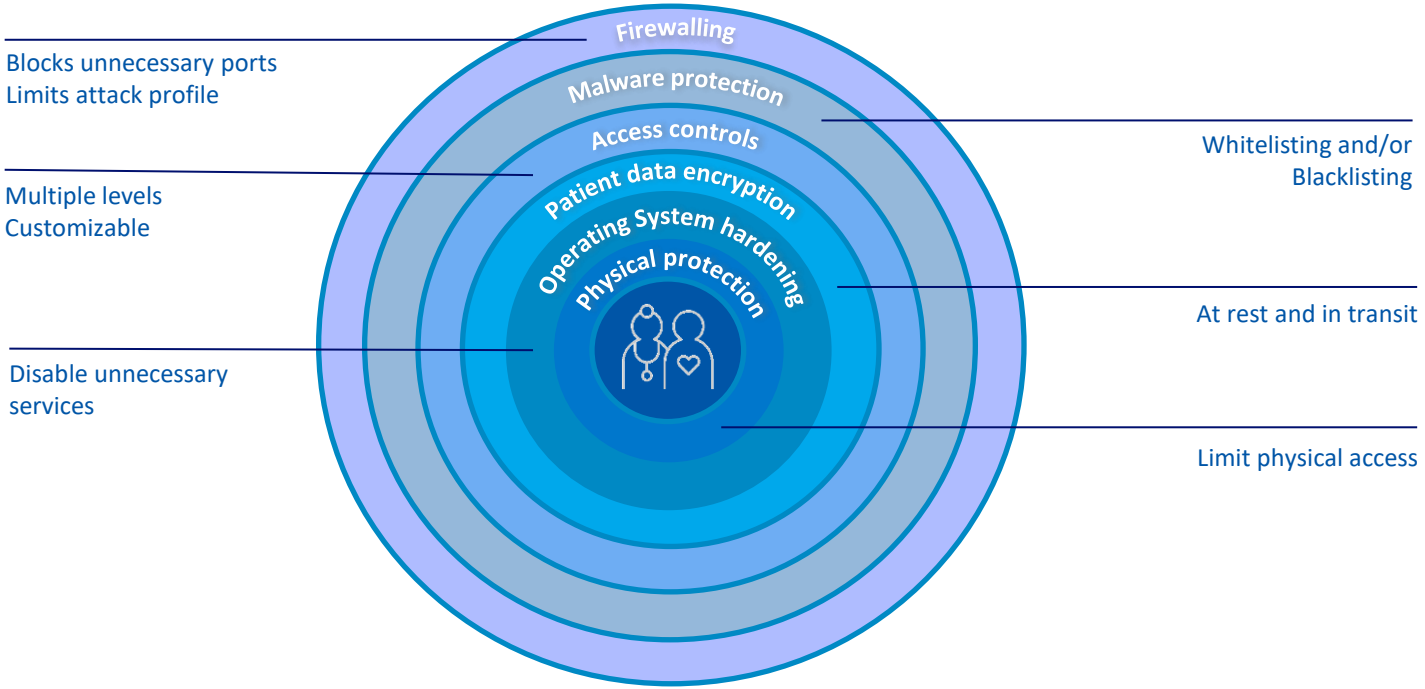


© Koninklijke Philips N.V.

PHILIPS

Philips’ defense in-depth strategy

Defense-in-depth strategy, the idea that a multi-layered defense is more difficult to penetrate than a single barrier, is the basis for best practices in medical device security. With Philips, hospitals and medical practices have the protection to keep health information and medical devices secure, giving patients true peace of mind.

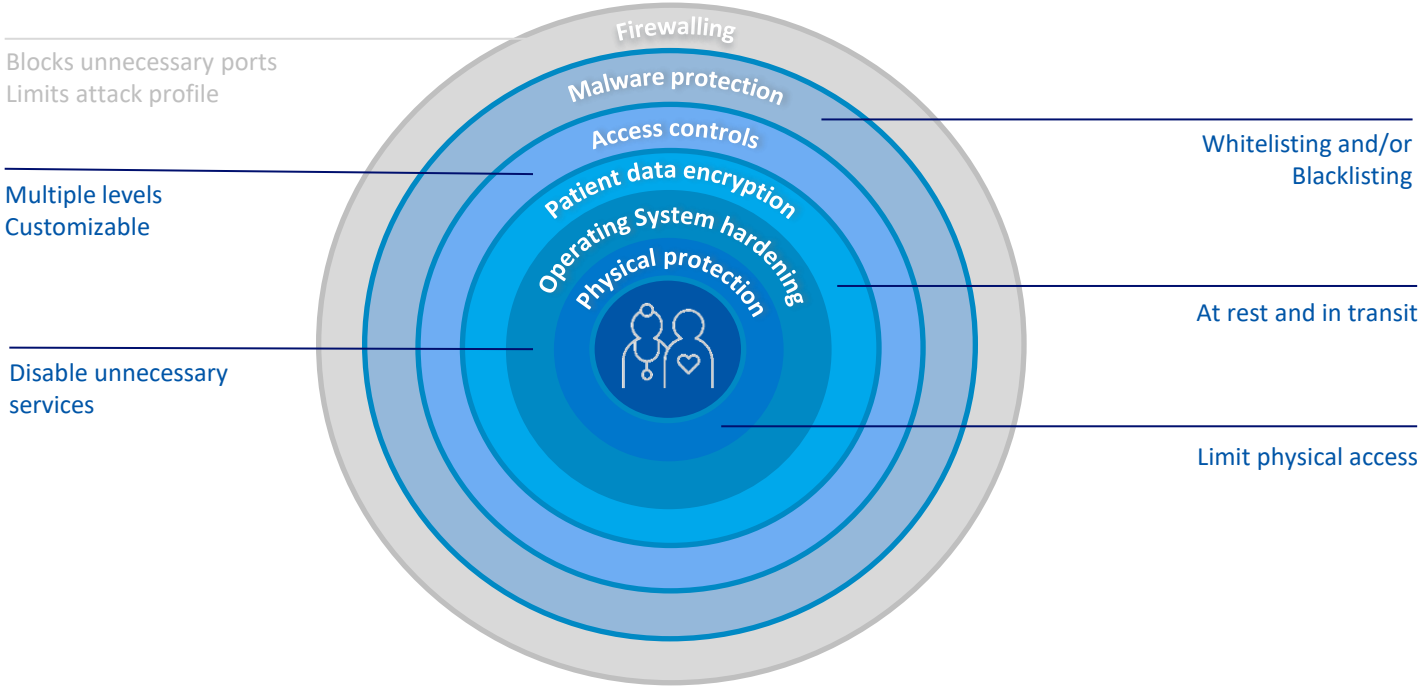


© Koninklijke Philips N.V.

PHILIPS

Philips’ defense in-depth strategy

Defense-in-depth strategy, the idea that a multi-layered defense is more difficult to penetrate than a single barrier, is the basis for best practices in medical device security. With Philips, hospitals and medical practices have the protection to keep health information and medical devices secure, giving patients true peace of mind.

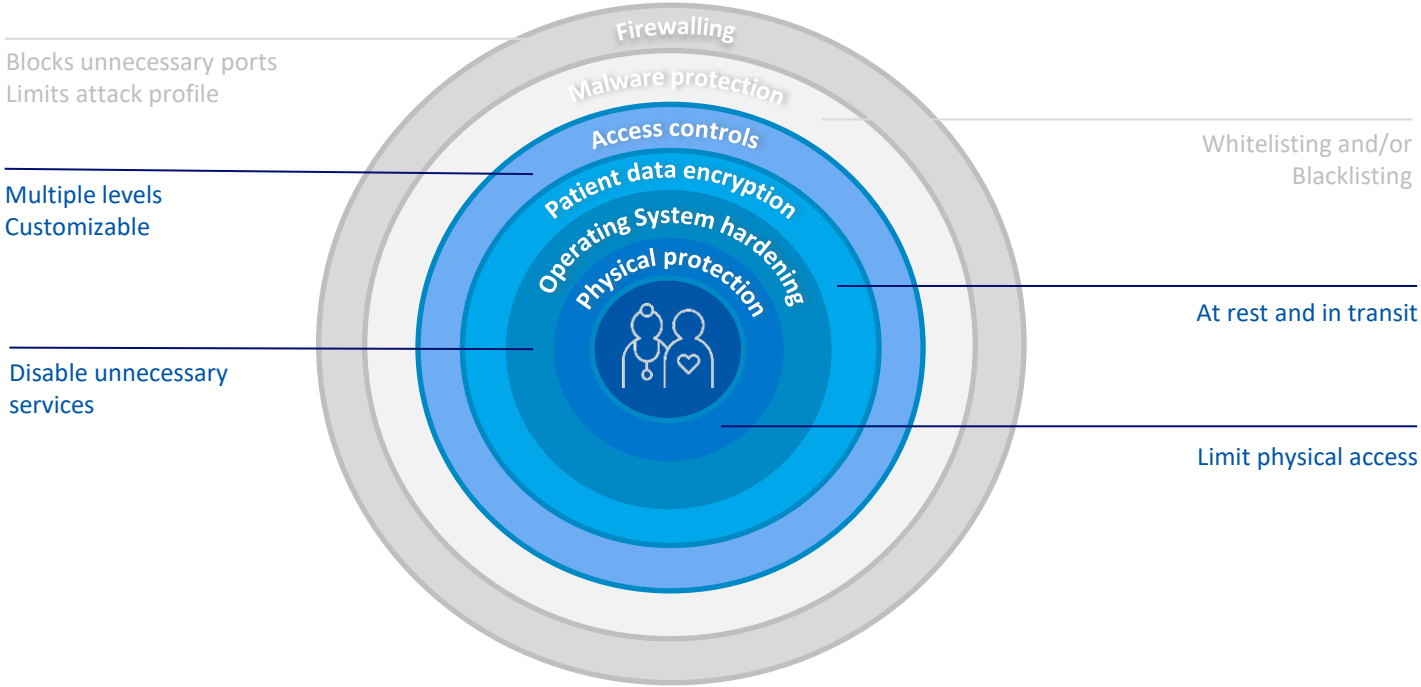


© Koninklijke Philips N.V.

PHILIPS

Philips’ defense in-depth strategy

Defense-in-depth strategy, the idea that a multi-layered defense is more difficult to penetrate than a single barrier, is the basis for best practices in medical device security. With Philips, hospitals and medical practices have the protection to keep health information and medical devices secure, giving patients true peace of mind.

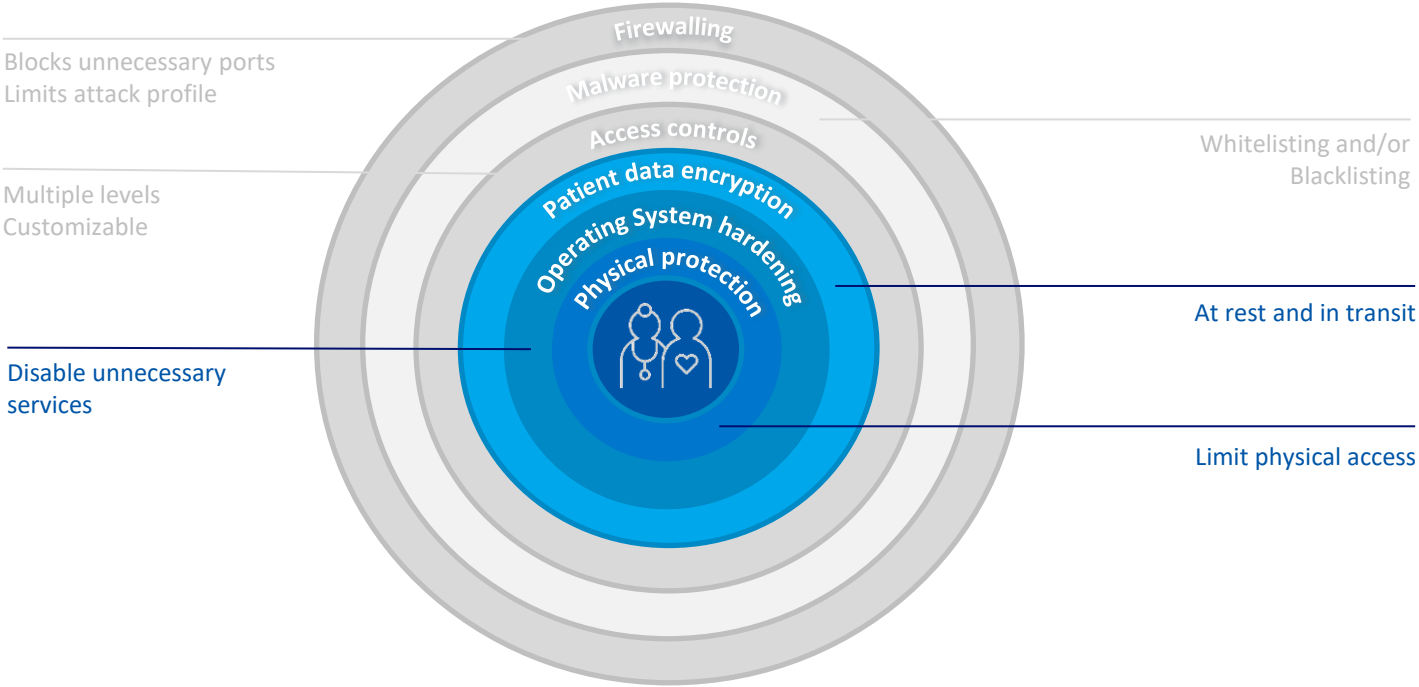


© Koninklijke Philips N.V.

PHILIPS

Philips’ defense in-depth strategy

Defense-in-depth strategy, the idea that a multi-layered defense is more difficult to penetrate than a single barrier, is the basis for best practices in medical device security. With Philips, hospitals and medical practices have the protection to keep health information and medical devices secure, giving patients true peace of mind.

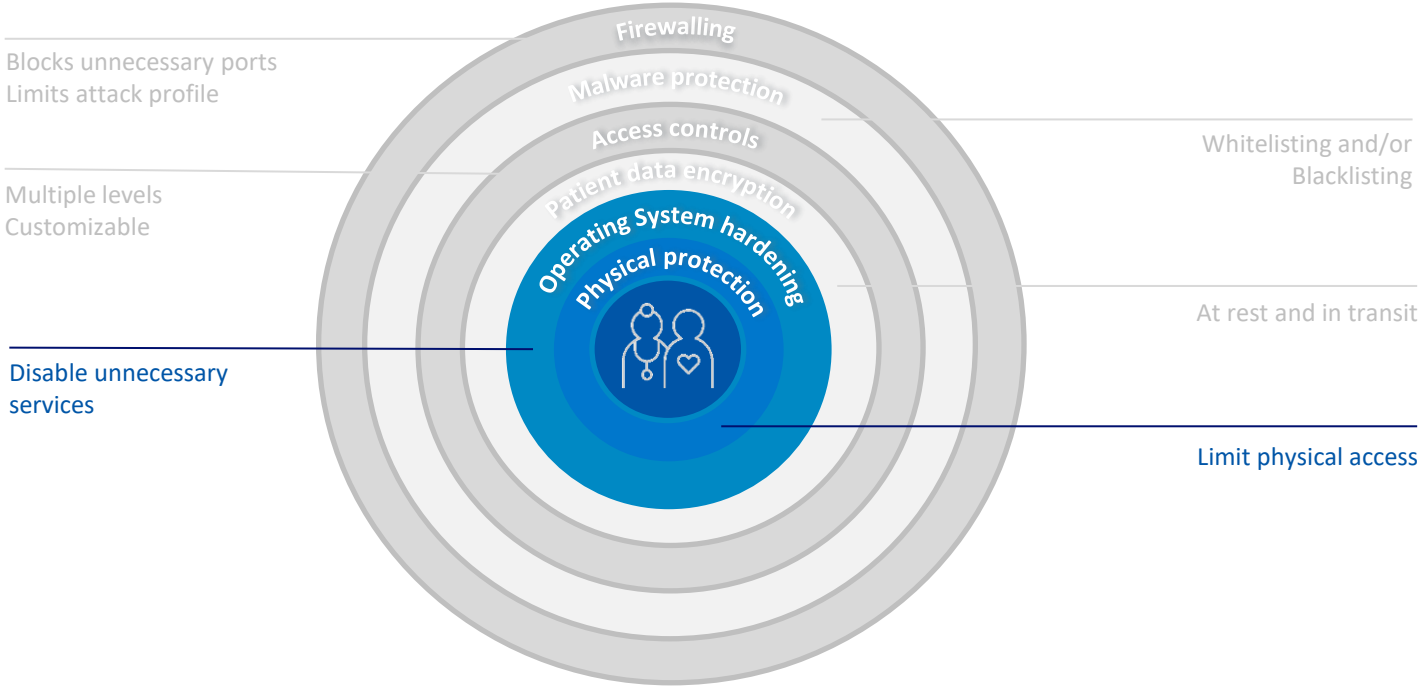


© Koninklijke Philips N.V.

PHILIPS

Philips’ defense in-depth strategy

Defense-in-depth strategy, the idea that a multi-layered defense is more difficult to penetrate than a single barrier, is the basis for best practices in medical device security. With Philips, hospitals and medical practices have the protection to keep health information and medical devices secure, giving patients true peace of mind.

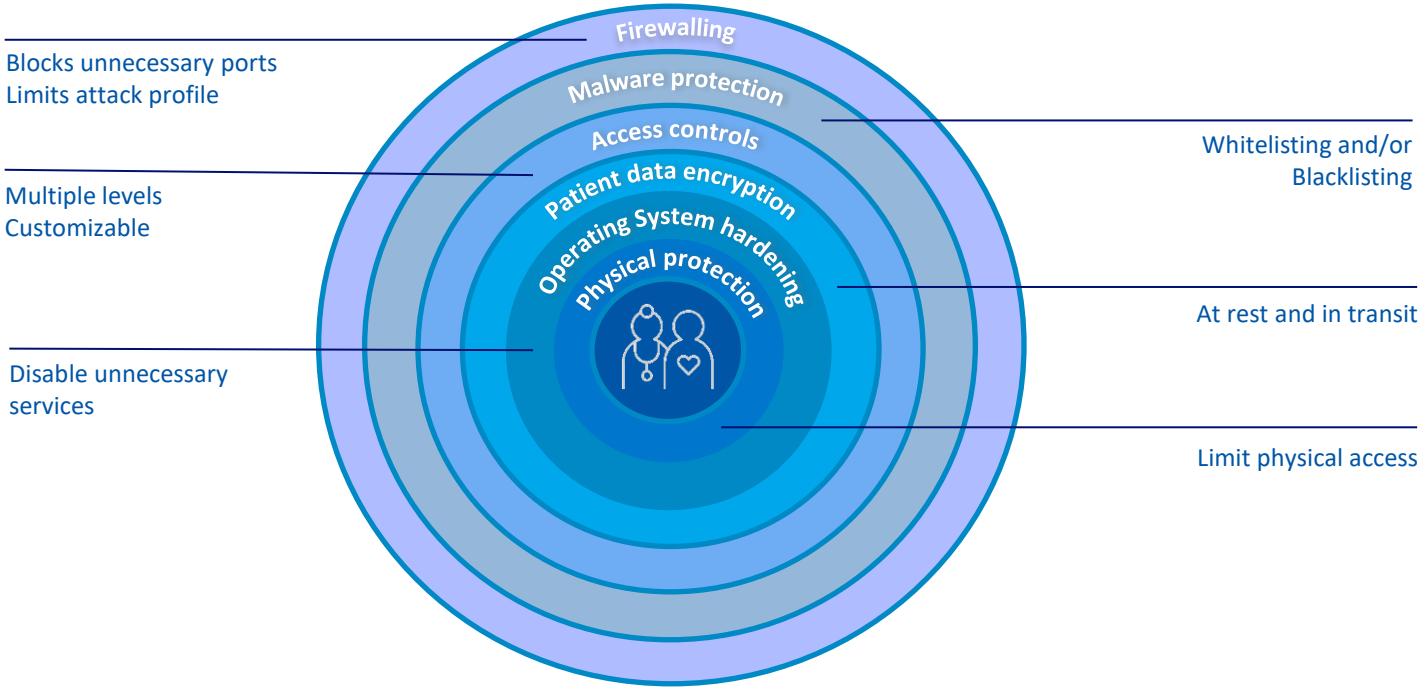


© Koninklijke Philips N.V.

PHILIPS

Philips’ defense in-depth strategy

Constantly evolving threat- and regulatory-landscape requires new security controls to be added when required

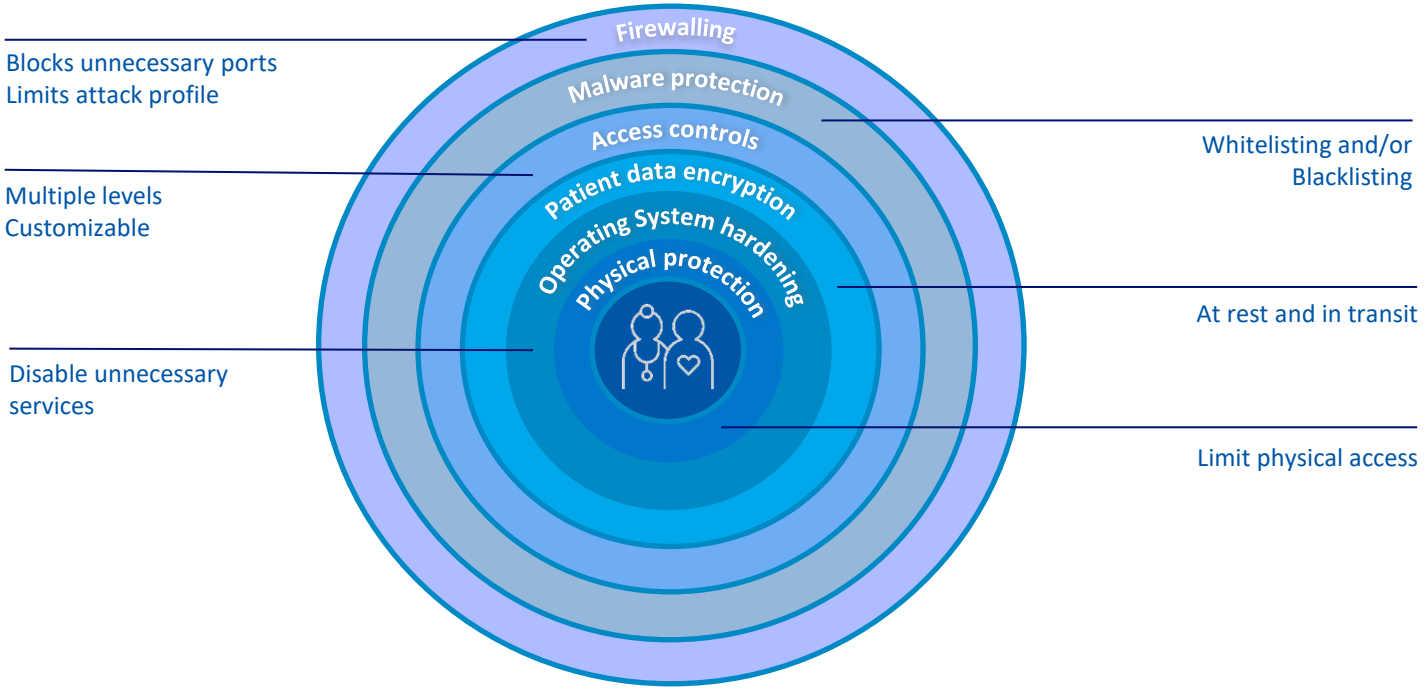


© Koninklijke Philips N.V.

PHILIPS

Philips’ defense in-depth strategy

Constantly evolving threat- and regulatory-landscape requires new security controls to be added when required

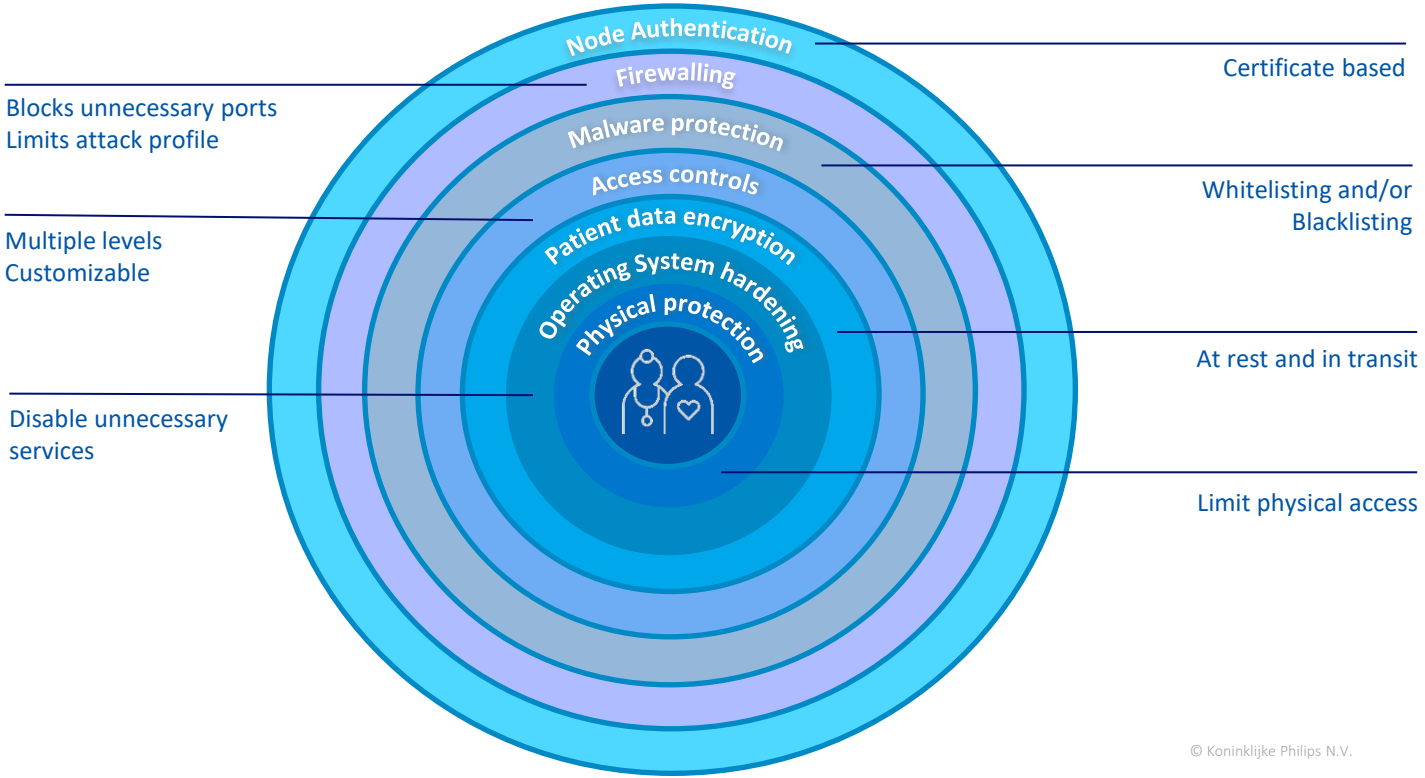


© Koninklijke Philips N.V.

PHILIPS

Philips’ defense in-depth strategy

Constantly evolving threat- and regulatory-landscape requires new security controls to be added when required

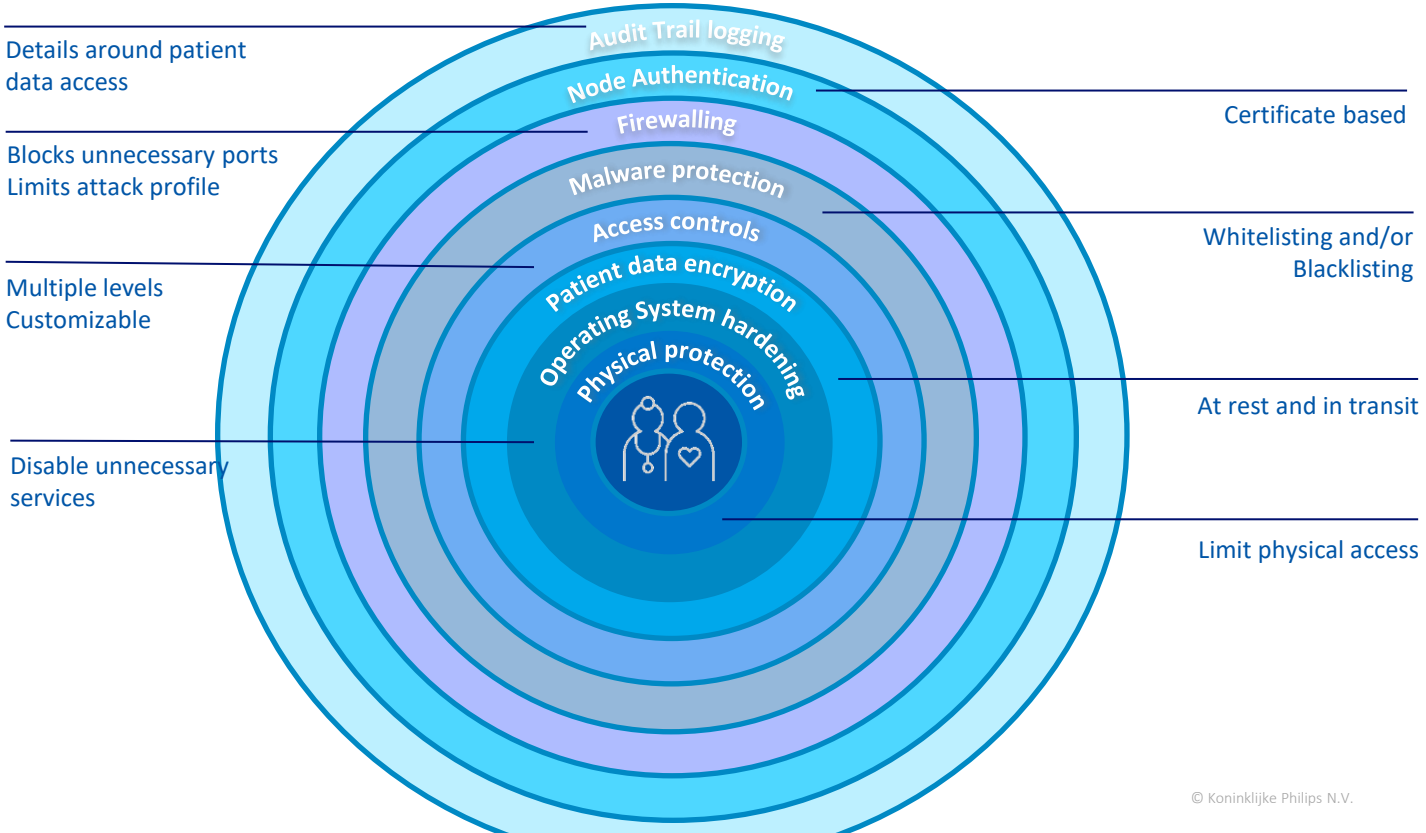


© Koninklijke Philips N.V.

PHILIPS

Philips’ defense in-depth strategy

Constantly evolving threat- and regulatory-landscape requires new security controls to be added when required

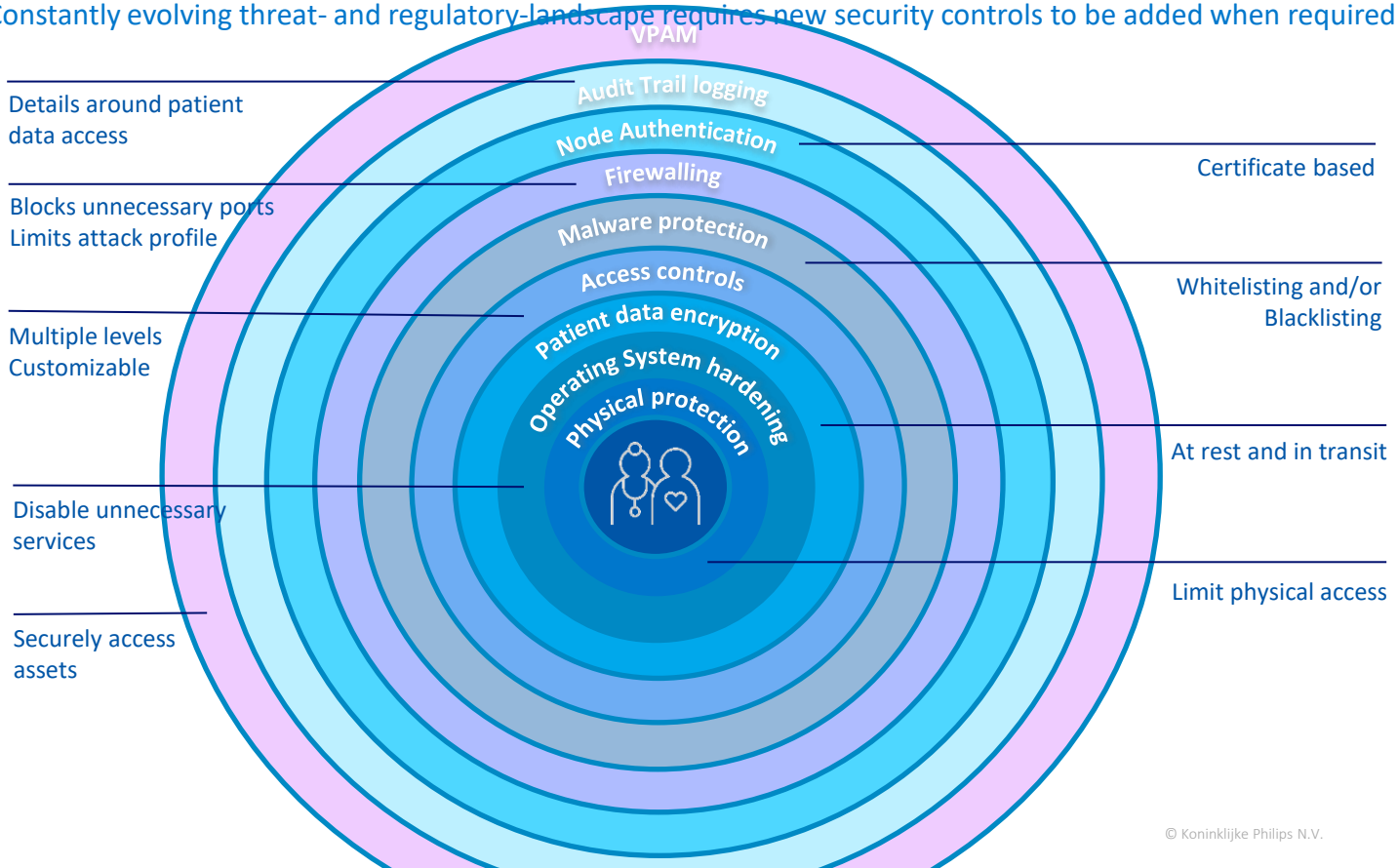


© Koninklijke Philips N.V.

PHILIPS

Philips' defense in-depth strategy

Constantly evolving threat- and regulatory-landscape requires new security controls to be added when required

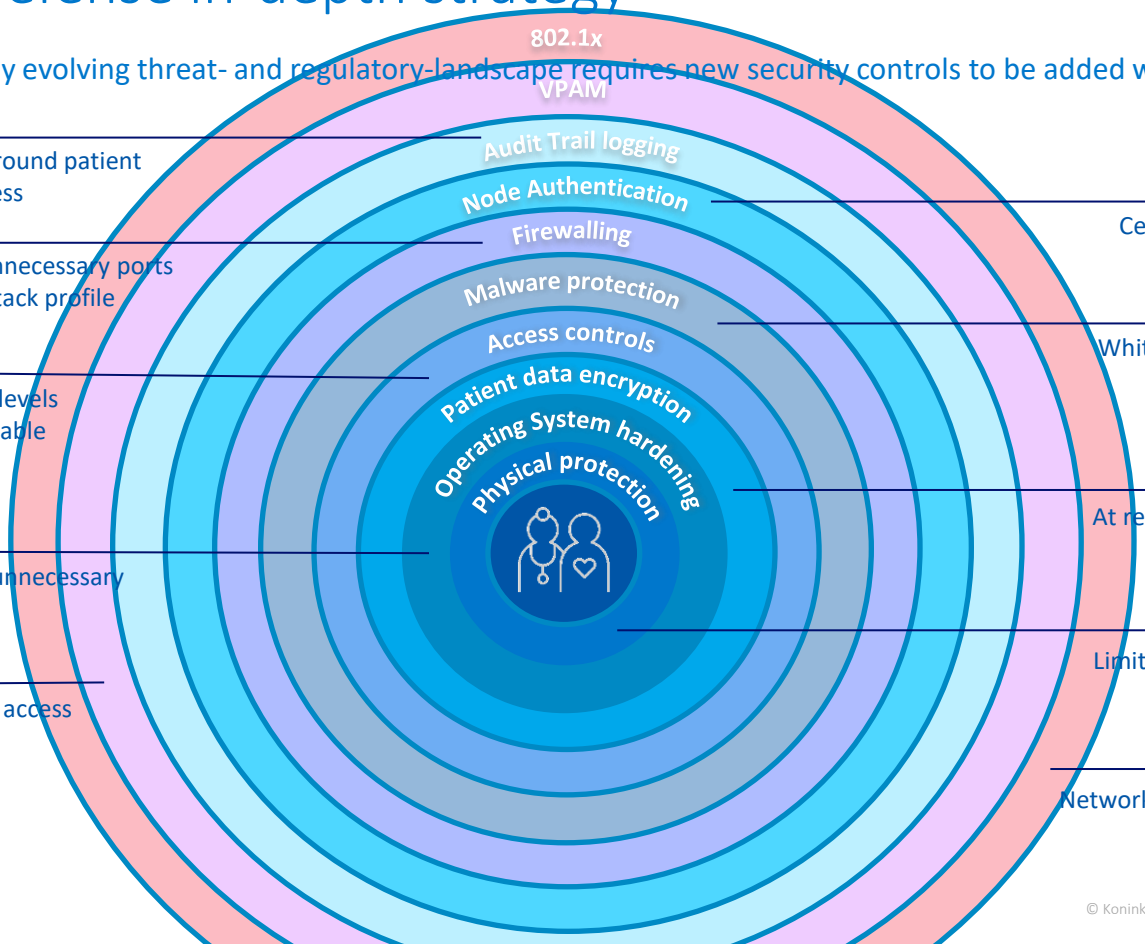


© Koninklijke Philips N.V.

PHILIPS

Philips' defense in-depth strategy

Constantly evolving threat- and regulatory-landscape requires new security controls to be added when required



Details around patient data access

Blocks unnecessary ports
Limits attack profile

Multiple levels
Customizable

Disable unnecessary services

Securely access assets

Certificate based

Whitelisting and/or Blacklisting

At rest and in transit

Limit physical access

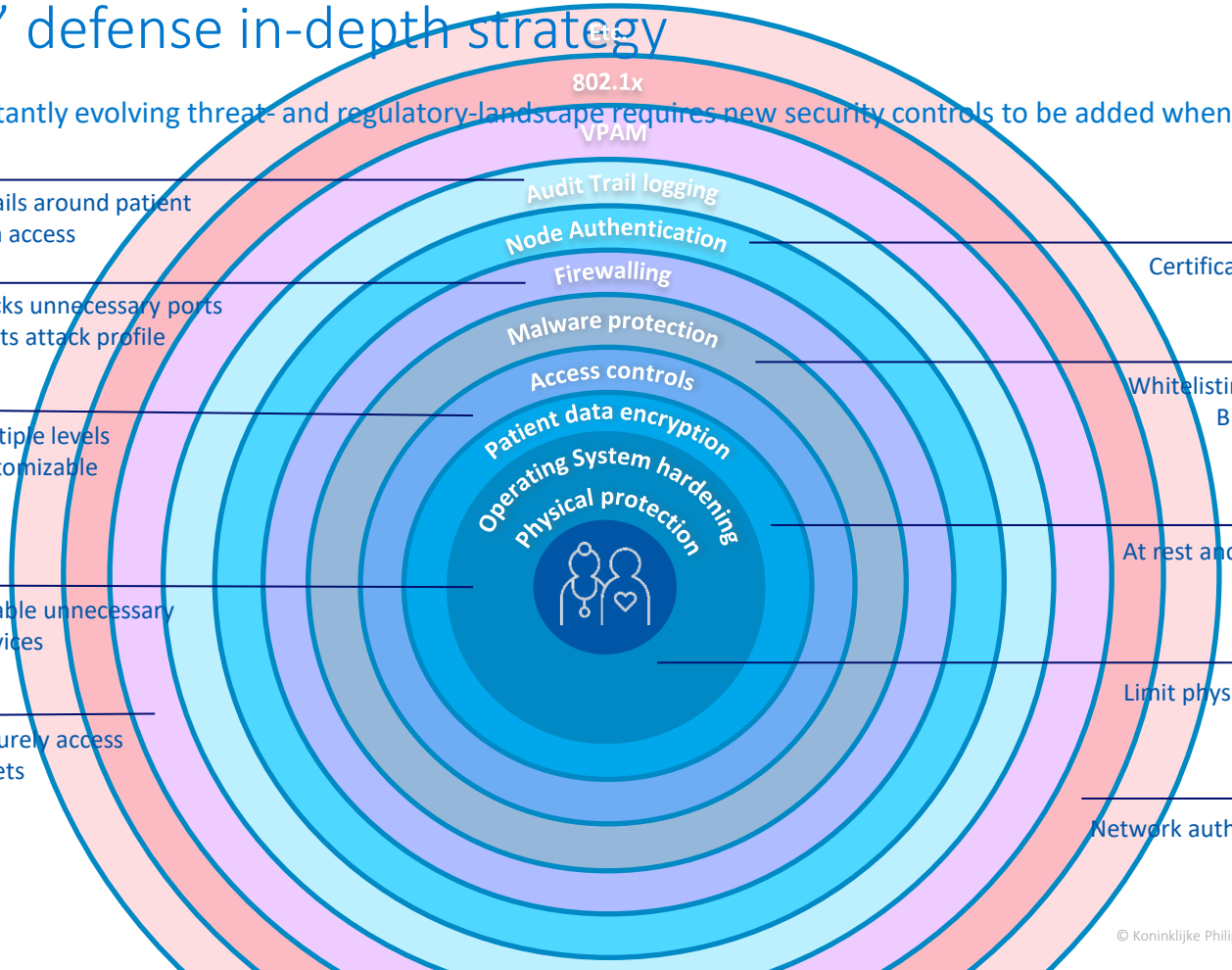
Network authentication

© Koninklijke Philips N.V.

PHILIPS

Philips' defense in-depth strategy

Constantly evolving threat- and regulatory-landscape requires new security controls to be added when required



Details around patient data access

Blocks unnecessary ports
Limits attack profile

Multiple levels
Customizable

Disable unnecessary services

Securely access assets

Certificate based

Whitelisting and/or Blacklisting

At rest and in transit

Limit physical access

Network authentication

© Koninklijke Philips N.V.

PHILIPS


Philips' Product Security Framework
CODE
DEPLOY
PLAN
BUILD
Pre-
Market
RELEASE
Post-
Market
OPERATE
TEST
MONITOR
Firewalling
Malware protection
Access controls
Patient data encryption
Operating System hardening
Physical protection

PHILIPS

How we communicate about security today

Manufacturer Disclosure Statement for Medical Device Security MDS2

Instructions for Use (Mandated Use, Residual Risk, etc.)

Security Status Document (Vulnerabilities, Patch Status, etc.)

DICOM Conformance Statement (Encryption-in-Transit)

Software Bill of Materials

Security Advisories



Labour intensive ?

© 2025 Koninklijke Philips N.V. All rights reserved.

PHILIPS

Cybersecurity Philips – Catharina Ziekenhuis

01

Aanleiding :

- Veel vragen en onduidelijkheden vanuit ziekenhuis MIT
- Regels, verantwoordelijkheden en risico's waren niet voor iedereen voldoende duidelijk

02

Actie :

- Organisatie van een conferentie binnen het ziekenhuis met een hoge opkomst (~100 deelnemers)
- Verduidelijking van de geldende regels en risico's
- Betrokken partijen met elkaar in contact gebracht om de samenwerking en wederzijds begrip te verbeteren

03

Vervolg :

- Diverse gesprekken gevoerd tussen ICT en Philips
- Screening uitgevoerd van de Catharina Installed base
- Security controls geïnventariseerd en gedocumenteerd

04

Risico's :

- Deze aanpak is niet werkbaar als deze periodiek moet worden herhaald.
- Er is behoefte aan een structureel en efficiënt proces dat voor alle betrokken partijen werkbaar is
- Zonder een duurzame oplossing bestaat het risico op terugkerende discussies




PHILIPS
Together
for a more resilient
healthcare future
From documents to real resilience
A shared responsibility for a more secure healthcare ecosystem
53%
of connected medical equipment has in average 6.2 vulnerabilities each
Medical Device Manufacturer
Shared Responsibility
Hospital
Current way of working
MDS2
Security Status Document
• Document-driven
• High workload
• Hospitals not sufficiently staffed
• Not scalable
• Need a more effective approach
Brainstorm
How can we improve?
- Shared responsibility model
- Reduce document burden
- Automate and integrate
- Continuous monitoring
- Clear roles and ownership
- Practical and scalable
- Stronger together
People
Process
Technology
Partnership
PHILIPS
MDS2
Security Status Document

PHILIPS

Do you want to participate in this brainstorm session ?
Please send an Email to: arno.vander.Heijden@philips.com

© Koninklijke Philips N.V.
PHILIPS

Questions ?



There are some viruses doctors can't treat.

© Koninklijke Philips N.V.

PHILIPS

PHILIPS