PHILIPS

Diagnostic X-ray

Protect your diagnostic X-ray systems with defense-in-depth

While the interconnected nature of medical devices and hospital IT networks has benefitted patient care, it has also increased the cybersecurity risk. To help you mitigate this risk, Philips has adopted a proactive approach to cybersecurity that begins during product development and extends long after devices are delivered to your hospital.

Our Plan, Do, Check, Act approach for processes associated with the creation, release, and maintenance of medical devices, including those that are part of our diagnostic X-ray product portfolio, helps us keep your equipment and data secure.

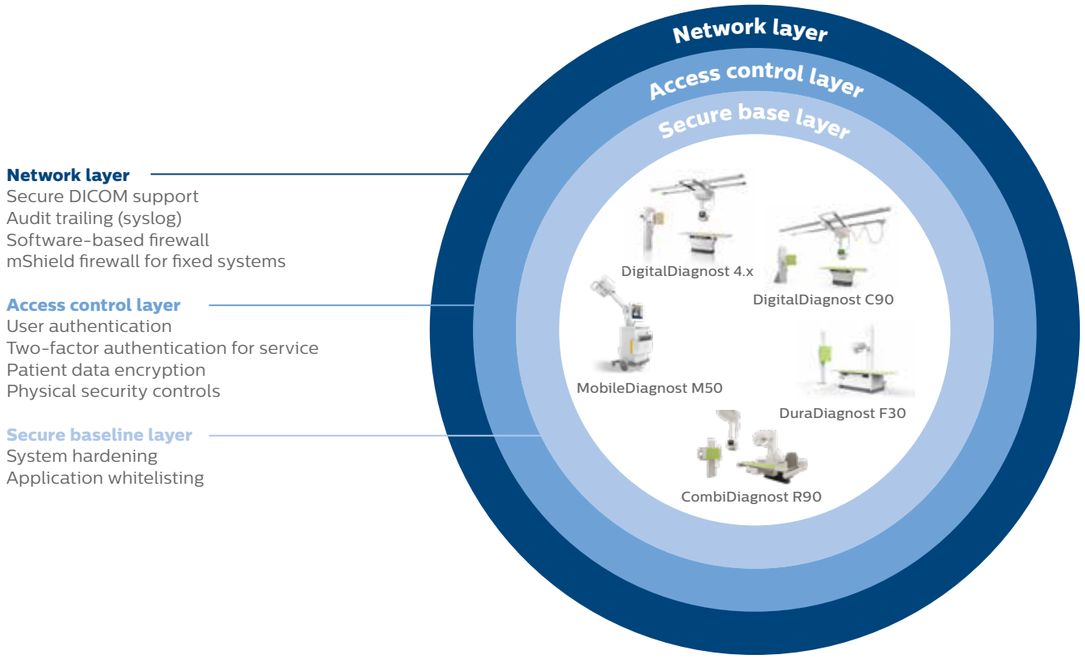
Cybersecurity in product design

For diagnostic X-ray systems, we have implemented a “defense-in-depth” strategy that uses security controls at various levels - application, computing, data, information, and network security – as well as administrative and operational safeguards. These security controls, which are derived from Philips Product and Services Security Policy and Security and Privacy Requirements for Products and Services (based upon IEC 80001 amongst other applicable standards and best practices), 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 security frameworks and standards worldwide, including - but not limited to - ISO 27001/27002/27018 and NIST SP 800-53.

Continuous monitoring
Our security and product experts evaluate the threat landscape associated with our diagnostic X-ray product portfolio on a regular schedule, as well as on an ad-hoc basis when merited by changes in the landscape. They evaluate vulnerabilities reported by suppliers and open source communities for integrated components. They also evaluate the applicability and related residual risk as identified during cybersecurity risk assessments[1] and internal penetration tests, or as reported via the Philips Coordinated Vulnerability Disclosure program for products in scope or equivalent products, as well as those legacy products still supported by Philips. You can access assessment outcomes and recommendations, as well as other cybersecurity related documentation, at https://www.philips.com/productsecurity.

Cybersecurity mitigations
We embed multi-layered cyber defense into our diagnostic X-ray products to prevent and reduce the likelihood of cybersecurity-related threats. These layers consist of technical measures based on industry best practices and applicable standards, and procedural measures and relevant guidance in product instruction for use documentation.

Security control	Control rationale
Software-based firewalls	Protect the system from network-based threats
Application whitelisting	Protect system integrity and block malware
System hardening	Limit access to the intended use of the medical device
Patient data encryption	Limit disclosure of data in case of HDD/PC theft
User authentication	Limit system access to authorized individuals
Two-factor authentication	Additional security for service level access
Support for secure DICOM	Protect the exchange of patient data with clinical image systems, e.g. PACS
Support for audit trailing (syslog)	Enable detection of potential misuse
mShield firewall for fixed systems	Commercial option to protect the system from network-based threats



Network layer
Secure DICOM support
Audit trailing (syslog)
Software-based firewall
mShield firewall for fixed systems

Access control layer
User authentication
Two-factor authentication for service
Patient data encryption
Physical security controls

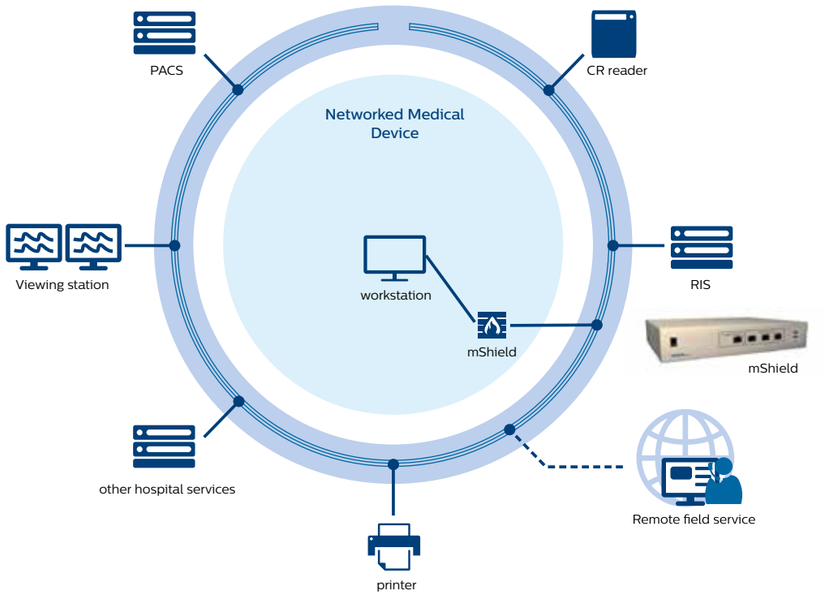
Secure baseline layer
System hardening
Application whitelisting

Network layer
safeguards against external threats

Secure DICOM protects the exchange of patient data
Information exchange between diagnostic X-ray equipment and PACS systems is encrypted using secure DICOM following the relevant DICOM standard[2]. Our systems leverage Transport Layer Security (TLS) for node authentication without encryption, DICOM utilizing TLS encryption, or a combination of the two to encrypt patient data in-transit. (This feature requires that nodes/PACS systems also support the relevant DICOM standard).

Audit trailing enables detection of potential misuse
Our diagnostic X-ray equipment supports audit logging capabilities following the relevant IHE standards[3] related to auditing and time synchronization. Important events such as login/logoff, patient data access and more are available on the device. They can be configured to forward these events to a central syslog server in your environment.

Software firewalls and mShield firewall protect your system from network-based threats
We configure and implement software firewalls to reduce the network-based attack surface of your X-ray systems. To further reduce the attack surface, we recommend the addition of optional mShield.[4] mShield is a physical firewall configured based on the intended use of your diagnostic X-ray equipment to safeguard normal system operation by network isolation, minimizing the connectivity exposure ("attack surface") between the medical equipment and the hospital's network. It limits traffic to only authorized devices and specific services. For example, diagnostic X-ray equipment typically uses DICOM as its primary communication protocol and only a few other supporting protocols. With a default-deny-policy and few firewall exceptions, mShield can effectively decouple the modality from the network and hide the modality's structure, while at the same time maintaining connectivity for medical applications or remote service. mShield can prevent malware replication over the network, ensure equipment availability, provide an additional layer of security, and offer security if the medical device's embedded operating system is no longer supported by the operating system's manufacturer. For more information on mShield, see the dedicated whitepaper.[5]



Learn more about how mShield protects your X-ray equipment against malicious activity here

Access control layer
protects the system from external access

User authentication and role-based access limits system access to authorized individuals
By defining users as clinical users, system administrators or Philips authorized service engineers and limiting the type of access accordingly, you can protect your X-ray equipment from unauthorized or accidental access. Clinical users are allowed to access the clinical applications and related functionality, while system administrators are able to conduct regular maintenance activities such as managing user, DICOM and networking-related configurations. Philips authorized service engineers are entitled to configure and update system software and have access to elevated service functions based on their entitlements and authorization level. For authentication, the equipment supports local accounts on the equipment as well as a coupling with central account management solutions via the Kerberos authentication protocol, which uses secret key cryptography. The exception is authentication for authorized Philips service engineers, which requires two-factor authentication using hardware dongles.

Two-factor authentication provides additional security for service level access
The two-factor authentication used by Philips authorized service engineers includes unique, person-bound dongles that have expiration dates and can only be re-activated by Philips. We plan to extend two-factor authentication to our customers, coupled to existing infrastructure, to some products in the diagnostic X-ray portfolio,[6] in the near future.

Patient data encryption limits disclosure of data in cases of breach
Diagnostic X-ray systems are not intended to serve as long-term storage devices for patient information and images. However, when patient imaging workload or network downtime interferes with timely export to PACS. To protect this data, we've applied an encryption at rest solution.

Physical access control protects your system from external devices
To prevent nefarious activity or unintentional harm from external devices such as USB drives or Bluetooth devices, we limit exposure of external interfaces to those required for normal system operation, and protect all others using system covers and other measures. Our instruction for use documentation contains recommendations about how to securely use the equipment, as well as recommendations for additional measures on both network and physical security aspects.

Secure baseline layer
provides a foundation of protection

System hardening limits access to services related to intended use
Similar in principle to firewalls, operating system hardening involves identifying all unnecessary services and functions included within the operating system and disabling those not required for the intended use of the diagnostic X-ray equipment. System hardening reduces the attack surface by eliminating those services that may become vulnerable over time. Philips follows the Standard Technical Implementation Guides (STIGs)[7] provided by the Defense Information Systems Agency (DISA).

Application whitelisting protects system integrity and blocks malware
Traditional anti-virus (AV) software depends on malware samples' availability and frequent updating of endpoints to protect against malware. Because diagnostic X-ray equipment cannot be frequently updated with causing considerable clinical downtime and because samples are only available after a breach, this malware protection method is ineffective for your X-ray systems. To proactively prevent malware infections, we embed application whitelisting into the equipment.

An inverse of the traditional AV technology, whitelisting enables us to permit software that we have validated and allowed explicitly. All other software, including malware, is blocked from the system. This proactive approach provides more control than traditional AV it can be configured only to allow the execution of software that is required under the intended use of the medical equipment. The whitelisting software only requires updates if a bug or vulnerability is detected in the solution itself. Whitelisting configuration changes are limited to software changes as part of product updates and upgrades and are validated and installed by trusted Philips installers.

Conclusion
This paper details current practices. Our product security personnel are committed to protecting your X-ray equipment from breaches of patient data, malware and other threats to system operation, and to staying abreast of new advances in cybersecurity. Should you have additional questions or wish to discuss your specific situation, please contact your local Philips representative.

1 Philips Coordinated Vulnerability Disclosure program details are available via following URL: https://www.philips.com/a-w/security.html

2 For more information on supported DICOM supplements/ standards see: https://www.philips.com/healthcare/resources/support-documentation/dicom-radiography

3 For more information on supported IHE standards see: https://www.philips.com/healthcare/resources/support-documentation/ihe-radiography

4 mShield is a commercial option for non-mobile X-ray systems, check with your sales representative for more information

5 For more information on mShield see the dedicated whitepaper on the following URL: https://www.usa.philips.com/c-dam/b2bhc/master/services/cybersecurity/DXR-philips-mShield-whitepaper.pdf

6 Two-factor authentication is not available on all products.

7 For more information on Security Technical Implementation Guides (STIGs) see following URL: https://public.cyber.mil/stigs/

4522 991 62171 * DEC 2020

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