PHILIPS

HealthSuite Imaging

Delivering secure cloud computing to protect data and enhance operations

Contents

Executive summary 3

Advanced security in the cloud 4

- Hybrid Cloud deployment 5
- Full Cloud deployment 5
- Web Application Firewall 6
- Virtual Private Cloud 6
- Security from the start: Product and service development 6
- Encryption in Transit 7
- Encryption at Rest 7
- Protection in Use 8
- Security Scan 8
- Endpoint Detection Response 8
- Data Resiliency 8
- Data Durability 8
- General product security 8
- Identity and Access Management (IAM) 9
- Multi-Factor Authentication (MFA) 9
- Zero Trust Security Architecture 9
- Centralized Logging and Immutable Audit Trails 9
- Secure Data Lifecycle and Deletion 9

Operational Security 10

- Event logging, auditing and monitoring 10
- Responding to cyber security threats 10

Conclusion 11

Executive summary

Philips is committed to delivering secure, private, and reliable imaging solutions that enable clinicians and radiologists to provide timely and confident diagnoses.

HealthSuite Imaging (HSI) embodies this commitment through its secure-by-design approach, leveraging the power of cloud computing to streamline image management, collaboration, and reporting. HealthSuite Imaging, our radiology cloud-based services, delivered as a SaaS solution, shifts the operational burden from healthcare providers to trusted partners—Philips and Amazon Web Services (AWS)—who ensure the platform is always up to date, monitored and compliant.

This document outlines the security principles, controls, and technologies embedded within the HSI cloud architecture to protect sensitive healthcare data and ensure operational integrity. It is intended to provide healthcare organizations, IT professionals, and decision-makers with a comprehensive view of how HSI safeguards patient and system information in a cloud environment.

Cloud computing brings new challenges and safeguards

Radiology departments face a demanding dynamic cybersecurity landscape due to their reliance on interconnected systems, constant availability, and high data throughput. Cloud-based platforms add new challenges that demand advanced safeguards—robust identity management, encrypted data storage, audit trails, and compliance controls—to ensure they don't become new entry points for attackers. Yet cloud-based solutions also bring significant improvements in security posture, simplifying upgrades and patching and centralizing and consolidating points of entry.

Introducing HealthSuite Imaging

Delivered as a Software as a Service (SaaS) solution, Philips HealthSuite Imaging (HSI) delivers a modular portfolio of Philips RIS and PACS services, ranging from exam scheduling, through patient registration, documentation, image processing and diagnostic interpretation to result distribution.

HSI provides a security-first architecture designed to mitigate the threats to data in the cloud. It shifts the operational burden from healthcare providers to trusted partners—Philips and Amazon Web Services (AWS)—who ensure the platform is always up to date, monitored and compliant. Security is embedded into every layer, from data encryption and access controls to vulnerability management and real-time threat detection. This enables healthcare IT teams to stay ahead of evolving threats without compromising system performance or clinical availability.

Advanced security in the cloud

HealthSuite Imaging benefits from a modern, robust cloud security framework that enhances protection well beyond the capabilities of traditional on-premises environments.

Each HSI instance is deployed in an AWS region selected by Philips based on its proximity to the healthcare provider, ensuring low latency and optimal performance. This architecture promotes fast access to imaging studies while maintaining compliance with local data residency and performance requirements. HSI utilizes the full range of AWS services to secure its infrastructure, including Amazon EC2, S3, ELB, VPC, IAM, KMS, CloudWatch, AppStream, Route53, WAF, and CloudTrail.

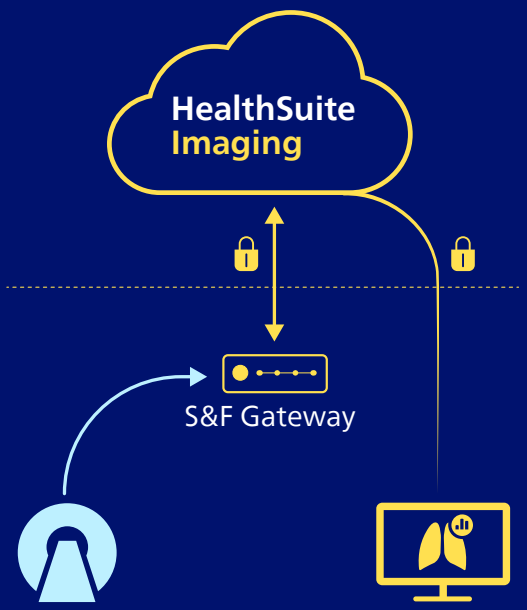
The cloud infrastructure is architected with strong network segmentation, isolating public-facing services (e.g., diagnostic viewers and enterprise portals) from backend services (e.g., databases and storage). Virtual Private Cloud (VPC) constructs, security groups and network access control lists (NACLs) are used to strictly control inbound and outbound network flows, ensuring secure and controlled access to all resources.

HealthSuite Imaging (HSI) is offered in 2 deployment modes:

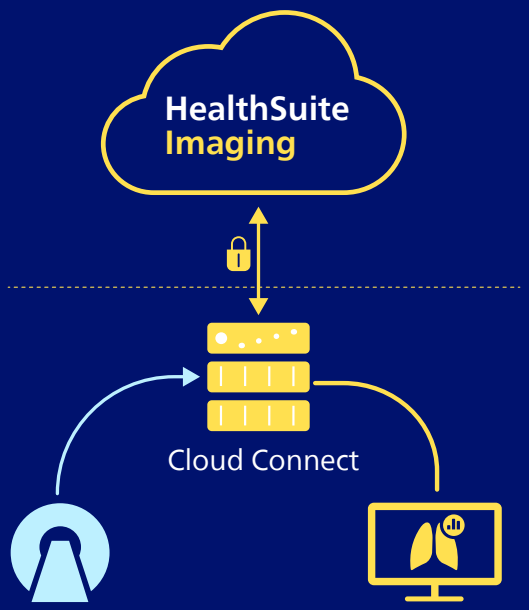
A HealthSuite Imaging Full Cloud Deployment is a setup where all medical imaging services are hosted entirely in the cloud. This means that the data and applications are stored and managed on remote servers, specifically on Amazon Web Services (AWS).

A HealthSuite Imaging Hybrid Cloud Deployment combines both on-premises and cloud-based components. This setup is well-suited for smaller healthcare providers or environments with lower network performance. It includes an on-premises device called Cloud Connect, which handles local data storage and quick access to images, while synchronizing data with a shared, multi-tenant environment in AWS

Full Cloud RIS and PACS Services



Hybrid Cloud PACS Services



Hybrid Cloud deployment

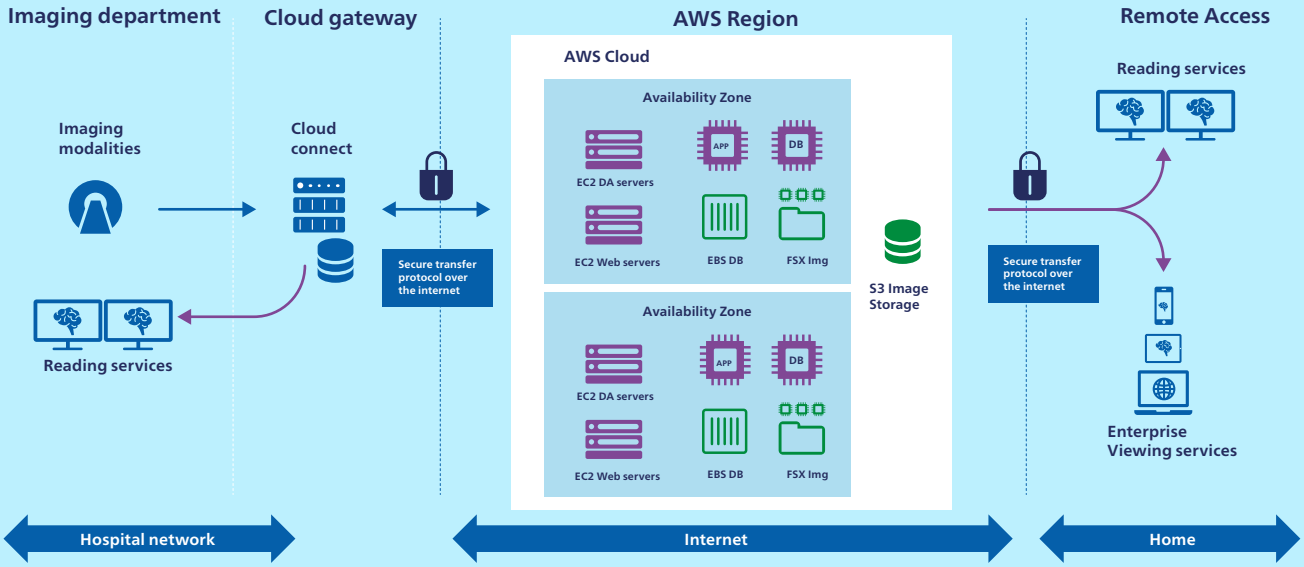


Figure 1: Hybrid Deployment

Full Cloud deployment

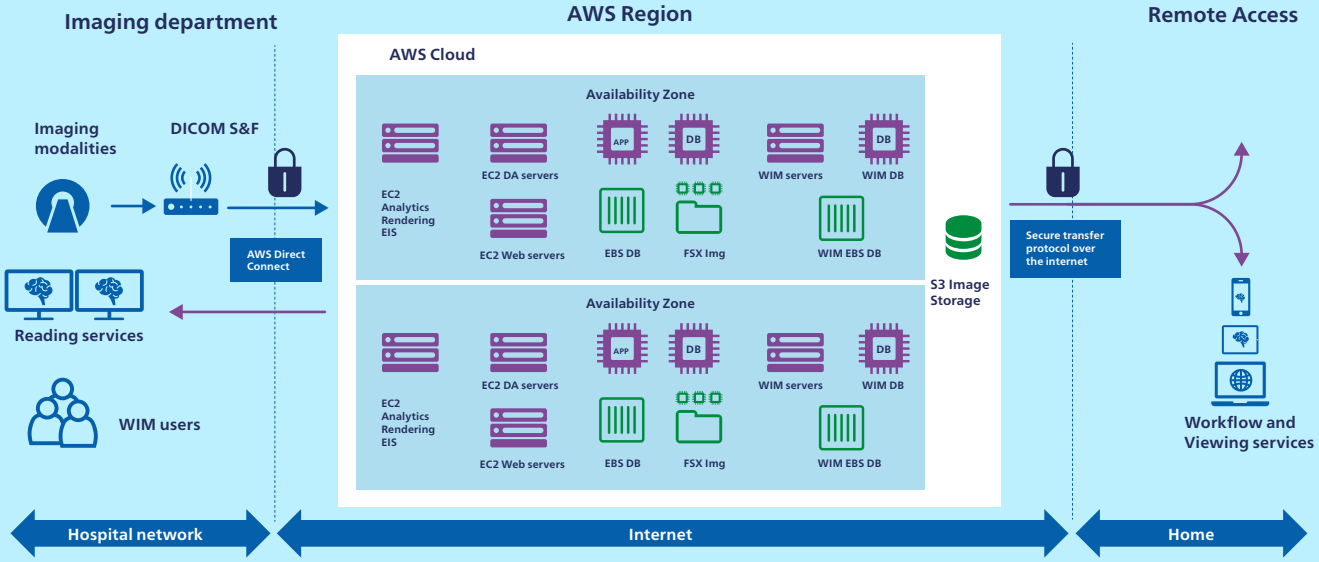


Figure 2: Full Cloud Deployment

With HSI Full Cloud deployment, each customer benefits from a dedicated instance on AWS, providing isolated and secure environments for their data and applications. This single-tenant model enhances security and performance, allowing for tailored configurations and optimizations specific to each healthcare provider's needs. To ensure efficient data transfer from modalities to the cloud, the architecture includes a DICOM Store and Forward system on-premises. This system facilitates the seamless forwarding of medical images to the cloud, ensuring that data is transmitted efficiently and reliably.

Web Application Firewall

HSI implements AWS Web Application Firewall (WAF) directly in front of the RIS and PACS web interfaces, such as the Enterprise Viewer and Diagnostic Client Gateway. WAF acts as a real-time defense layer against malicious traffic, shielding the system from common web exploits, bot activity, denial-of-service attempts, bad reputation IP's, cross site scripting and SQL injections.
By inspecting HTTP/S traffic before it reaches the application layer, AWS WAF preserves the availability and integrity of the system while ensuring only legitimate users can access critical clinical interfaces.

Virtual Private Cloud

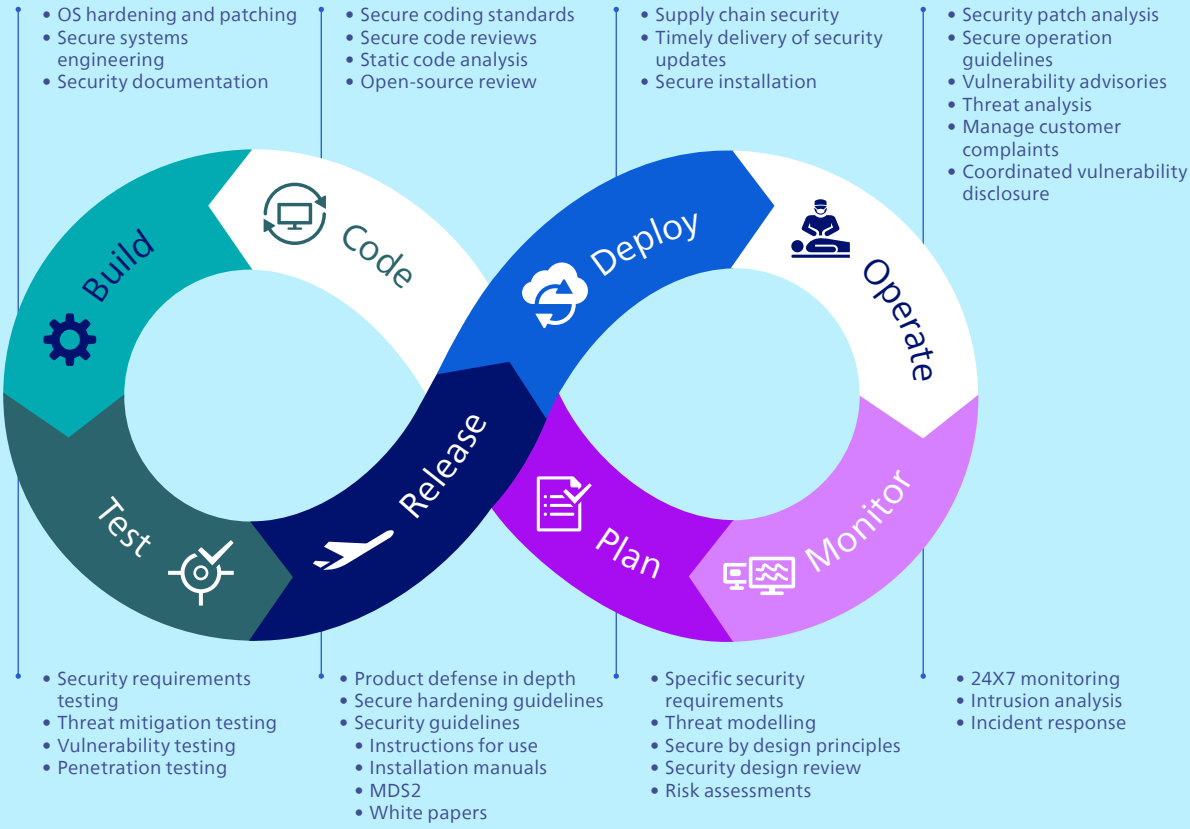
The AWS Virtual Private Cloud (VPC) architecture adopted for each HSI customer strictly segments public-facing services and internal components. Access to user-facing systems such as the diagnostic viewer is isolated, while backend systems—including databases and archives—are confined to private subnets inaccessible from the internet. This layered approach ensures sensitive data remains protected, reducing exposure and enabling fine-grained control over internal network flows.

Security from the start: Product and service development

Philips integrates cybersecurity into every phase of product and service development using a comprehensive Product Security Framework aligned with global security standards. This framework, applied across all Philips software products, encompasses structured activities such as Product Security Risk Assessments (PSRA), secure architecture and design, vulnerability and penetration testing, and security training across the organization.

Beyond Technological Threats

Philips applies a mature Information Security Management System (ISMS) to protect the business of customers, to meet the objectives for confidentiality, integrity and availability (the "CIA triad") of the data and the service. The ISMS is based on a holistic approach to information security, where the measures to mitigate risks cover organizational, people, physical and technological controls.
The continuing adequacy of the ISMS to meet its security objectives is assessed annually with internal audits by an independent organization within Philips, as well as externally by the accredited bodies to maintain the information security certifications (see below).



Encryption in Transit

All communication across the HSI platform is encrypted using modern protocols that align with healthcare industry standards. Within the cloud environment, internal services communicate using proprietary protocols secured with Transport Layer Security (TLS), preventing unauthorized interception or manipulation of data.

In HSI full cloud implementation:
Communication with medical imaging devices, HSI supports DICOM TLS, ensuring encrypted and authenticated data exchange between trusted imaging systems. All web-based interfaces and applications use HTTPS secured with TLS 1.2 or above, offering robust protection for browser-based access to imaging and reporting tools.

When connecting on-premises environments to the cloud, the system leverages AWS Direct Connect (DX), which is enhanced with MACSec encryption. This protocol provides confidentiality and integrity at the network level (Layer 2), ensuring that any data transmitted between the healthcare facility and the cloud is secured by default—even before application-level encryption is applied. This layered approach ensures that personal health data remains protected throughout its journey.

In HSI hybrid cloud implementation:
The connection between the on-premises environment and the cloud is secured using a VPN tunnel, established by an SSL appliance device, using the AES-256-CBC cipher for encryption and SHA256 message hash for HMAC authentication. This encrypted communication channel leverages Transport Layer Security (TLS) to ensure data confidentiality and integrity during transmission.

Encryption at Rest

HSI applies strong encryption to all stored data, including both metadata and imaging content, to protect it from unauthorized access. Database credentials, certificates, and encryption keys are managed securely through Oracle Wallets, with access restricted to the Philips service team.

AWS native storage services such as S3, EBS, and FSx, provide built-in encryption capabilities for imaging data and associated files. These services use the AWS Key Management Service (KMS) with customer-managed keys (CMK) that are controlled exclusively by Philips. Each customer's data is encrypted with a dedicated key, ensuring strong separation and confidentiality.

Locally attached storage on EC2 instances, FSx for Windows file systems and Amazon S3 buckets are all encrypted using AES-256 keys managed through AWS KMS. Access to these keys is tightly controlled with granular policies that define which Philips service components can decrypt data. This approach prevents AWS from being able to access the content of encrypted volumes or objects. Furthermore, credentials and private keys are not accessible by AWS but are managed by Philips to further reduce exposure.

Additional safeguards include automated key rotation, comprehensive audit logging via AWS CloudTrail and strict access control policies enforced through AWS IAM. These measures ensure that access to encrypted data is always auditable and limited to authorized personnel only.

Protection in Use

In addition to encrypting data at rest and in transit, HSI also protects data while it is being processed. This is made possible through the AWS Nitro System, which is the foundational security layer behind Amazon EC2 instances. Nitro prevents even AWS personnel from being able to access customer data inside virtual machines.

Unlike traditional cloud systems, Nitro was designed from the ground up to eliminate operator access, meaning there is no backdoor or administrative override that can be used to view or retrieve customer content. This unique security model was independently validated in a 2023 audit by the NCC Group, which confirmed that Nitro does not provide any mechanism for AWS employees to access data on Nitro-based hosts.

By deploying HSI on Nitro-based infrastructure, Philips ensures that customer data is shielded from external and internal threats, including those originating from the cloud provider itself. This additional layer of protection is particularly valuable for healthcare organizations concerned with the privacy of sensitive patient information, providing confidence that even during data processing, no unauthorized access is possible.

Security Scan

To proactively identify and mitigate vulnerabilities, HSI integrates security scanning tools. These services regularly assess the environment for misconfigurations, compliance drift and potential security threats. Alerts are prioritized and aggregated to support timely remediation. These automated assessments complement manual reviews and contribute to a continuously monitored security posture.

Endpoint Detection Response

Trend Micro's Endpoint Detection and Response (EDR) solution fortifies endpoint security on EC2 instances. EDR provides real-time monitoring, threat detection and rapid response capabilities for all compute endpoints, so the systems hosting PACS components are continuously checked for abnormal behavior and remediation can be swift if any compromise is suspected. The Philips Security Operations Center (SOC) is monitoring the install base on a 24/7 basis.

Data Resiliency

Amazon S3's enables the recovery of previous object states, preventing data loss due to accidental deletions or overwrites. Object Lock enforces a Write Once Read Many (WORM) policy, ensuring that medical imaging data cannot be altered or removed for a defined retention period. These safeguards are enabled by default for all archived imaging data, supporting a reliable and immutable archive strategy.

Data Durability

HSI leverages the 99.999999999% (11 nines) durability of Amazon S3 to ensure long-term data preservation. S3stores data redundantly across multiple Availability Zones within an AWS region. The PACS software intelligently selects the most appropriate storage tier based on access patterns, optimizing cost-efficiency while ensuring rapid availability for both recent and historical studies.

General product security

All the services available as part of the HealthSuite Imaging portfolio are developed following the comprehensive security framework established for Philips Radiology Informatics solutions. To learn more about the Philips security framework, please reference the white paper, Cybersecurity in Radiology Informatics, which you can find at https://www.usa.philips.com/healthcare/white-paper/cybersecurity-for-radiology-informatics or by asking your Philips radiology informatics representative. This white paper provides in-depth explanations of Philips security in terms of:

- Industry Standards and Compliance
- Third-Party and Supply Chain Security
- Malware Protection and OS Patching
- System Hardening and Data Security
- Application-Level Security
- Secure Remote Access
- User Management
- Business Continuity and Disaster Recovery
- Threat Monitoring and Incident Response

Want to learn more? Visit (Link to whitepaper)

Identity and Access Management (IAM)

AWS IAM enables precise control over who/what can access which resources and under which conditions. Each service, account and user is governed by a principle of least privilege, ensuring that individuals and systems only have the permissions strictly necessary to perform their designated functions. Role-based access control (RBAC) is used extensively to define access boundaries across user types—administrators, radiologists, IT operators and integration partners—providing both security and operational clarity.

Multi-Factor Authentication (MFA)

To protect sensitive access points, administrative access to cloud infrastructure requires multi-factor authentication (MFA). By requiring a second authentication factor—typically a mobile token or biometric confirmation—MFA adds a critical layer of defense against compromised credentials. This is especially vital in a healthcare environment, where the integrity of medical data and system availability are non-negotiable.

HSI full cloud deployment supports integration with hospital identity systems via SAML, enabling streamlined and secure user access management. Support for OpenID Connect is planned for future enhancements, further expanding identity federation capabilities.

For HSI hybrid the Enterprise viewing web portal supports MFA through a one-time password.

Zero Trust Security Architecture

With HSI's zero trust security, no user or system is inherently trusted, whether inside or outside the cloud perimeter. Verification is required at every access point and trust is established dynamically based on device posture, network location and credential strength. This approach complements existing segmentation and access controls, reducing the risk of lateral movement in the event of a breach.

Centralized Logging and Immutable Audit Trails

HIS's comprehensive logging and monitoring supports operational oversight and forensic readiness. All activity is logged using AWS CloudTrail and centralized in a secure log store. These logs are protected against tampering and support detailed audit trails, which are crucial in regulatory and incident response contexts. Optional log immutability can be enabled to ensure Write Once Read Many (WORM) protections, further enhancing compliance readiness.

Secure Data Lifecycle and Deletion

From ingestion to archival and eventual deletion, HIS governs data flows through policies that ensure both availability and compliance. When data reaches the end of its retention period, deletion routines ensure it is removed securely and irreversibly.

Operational Security

The Philips service and operations team, operating within leading practices and adherence to ITIL (Information Technology Infrastructure Library) framework, continually evaluate security risks, privacy risks and controls during HealthSuite Imaging operation and maintenance to minimize risks and maximize availability.

Event logging, auditing and monitoring

Regulations require organizations to log all activities concerning Protected Health Information (PHI). Each logged event can include warnings and failures, operation performed, user who performed it, location from which it occurred (including the client's IP) and the information affected (including the study instance unique identifier).

An audit is an event log that collects important actions and events in the system for the purposes of tracking and investigating past actions in the system. It is a write/read only table, which means Philips can only write to it and read the information afterwards. Once created, it is never edited or deleted.

Log and audit trails are crucial in cybersecurity because they provide a detailed record of system activities, allowing for the detection of security incidents, investigation of suspicious events, compliance with regulatory requirements and analysis of historical data to improve security posture and response strategies.

Philips can provide detailed audit trail logs that are IHE ATNA compliant, which apply to logging on, reading and modifying clinical information.

Audit trail logs are either stored locally (in an encrypted form) on the system or transferred to a central Syslog server. Hospital administrators can monitor logged events stored locally and identify unusual system activity or suspicious user behavior using the Audit Log Viewer. They can then filter records according to their needs and export if necessary.

Responding to cyber security threats

The top priority of the 24/7 Philips Security Operations Center (SOC) is safeguarding the security of vital assets such as the Vue PACS and Image Management Software Our multifaceted strategy integrates proactive measures such as continuous monitoring and threat detection, leveraging state-of-the-art technologies.

In the event of an incident, Philips Imaging Informatics SOC, rapid triage and containment procedures swiftly isolate affected systems to mitigate harm and prevent the spread of the threat. Analysts delve deep into forensic evidence, log data and network traffic to grasp the attacker's tactics, techniques and objectives. This granular analysis informs our response strategies and enhances our threat detection capabilities, enabling us to anticipate and thwart future threats more effectively.

Philips maintains open channels of dialogue with internal stakeholders, external partners and regulatory bodies to keep all relevant parties informed throughout the incident response process. This collaborative ethos extends to our remediation efforts; we work tirelessly to restore affected systems to a secure state. From patching vulnerabilities and deploying security updates, to resetting compromised credentials and restoring data from backups, our focus remains steadfast on safeguarding critical assets and maintaining operational continuity.

Post-incident analysis provides invaluable insights into areas for improvement. Thorough assessments identify gaps in security controls, weaknesses in incident response procedures and opportunities for enhancement. Philips commitment to continuous improvement includes ongoing investment in training and skill development to ensure that analysts remain at the forefront of cybersecurity best practices.

Conclusion

HealthSuite Imaging is purpose-built to support secure, scalable and high-performance diagnostic imaging in the cloud. Its architecture integrates advanced security technologies, strong governance, and a secure-by-design approach to protect patient data, meet regulatory expectations and enable clinical efficiency. From identity management and encryption to continuous threat detection and structured incident response, every aspect of the platform is engineered with security as a foundational principle.

Philips maintains a proactive approach to security, incorporating regular updates, independent assessments and third-party certifications to ensure HealthSuite Imaging continues to evolve alongside the dynamic threat landscape. The security controls are continuously tested and validated against industry benchmarks and healthcare-specific cybersecurity standards.

As cybersecurity challenges grow in complexity, Philips remains committed to maintaining the trust of healthcare providers and patients by delivering secure, resilient and compliant solutions.

Get in touch

Interested to learn more?

We'd love an opportunity to discuss how we can partner to create solutions and services to address your specific needs. Please get in touch with Philips Radiology Informatics.

1 Neitzel E, vanSonnenberg E, Markovich D, Parris D, Tarrant J, Casola G, Mamlouk MD, Simeone JF, The New Normal or a Return to Normal: Nationwide Remote Radiology Reading Practices after Two Years of the COVID-19 Pandemic Journal of the American College of Radiology (2023), doi: https://doi.org/10.1016/j.jacr.2023.04.014.

00001167-00-00 * SEPT 2025

How to reach us
https://www.usa.philips.com/healthcare/service/healthsuite-imaging-cloud-pacs