White Paper

The Zero Trust Blueprint for the Modern Hospital

Architecting patient-centric security with Netskope One and a connected partner ecosystem.

netskope

Building a digitally secure hospital

Modern healthcare environments are more connected—and more exposed—than ever before. As hospitals and their networks of connected healthcare services expand their digital footprint, traditional security models struggle to keep pace.

In this eBook, we outline why the transition to a zero trust mindset and access architecture is essential to modern healthcare security, and we'll explain how to do it in a way that feels achievable and not overwhelming.

With a SASE solution, and its security component, security service edge (SSE) as the foundation, organizations can build digitally secure hospitals and healthcare service provision. This approach enables seamless connectivity across the broader healthcare ecosystem, supporting secure data exchange with partner healthcare providers for patient-centered care and improved outcomes. With the right blueprint in place, digital enablement becomes smoother and faster.

Table of Contents

1. INTRODUCTION: WHY HOSPITALS NEED A ZERO TRUST BLUEPRINT NOW

Modern hospitals are vast data factories, processing extraordinary volumes of sensitive information every day. A single intensive care unit (ICU) patient generates over 1,000 data points daily, from vital signs monitored by bedside equipment, to test results, images, and clinical notes. Adoption of AI-driven diagnostics, clinical decision support tools, and automated workflows has also led to all kinds of new forms of processing and analysis of this data.

When these factors are applied across an entire hospital with hundreds of patients and dozens of different software applications, the data ecosystem becomes increasingly fractured and complex. The concentration of protected health information (PHI) and other valuable data, combined with expanding digital infrastructure and AI integration, has turned hospitals into prime targets for cyber criminals, while also increasing exposure to insider threats, shadow AI usage, and the risks of data leakage and exfiltration.

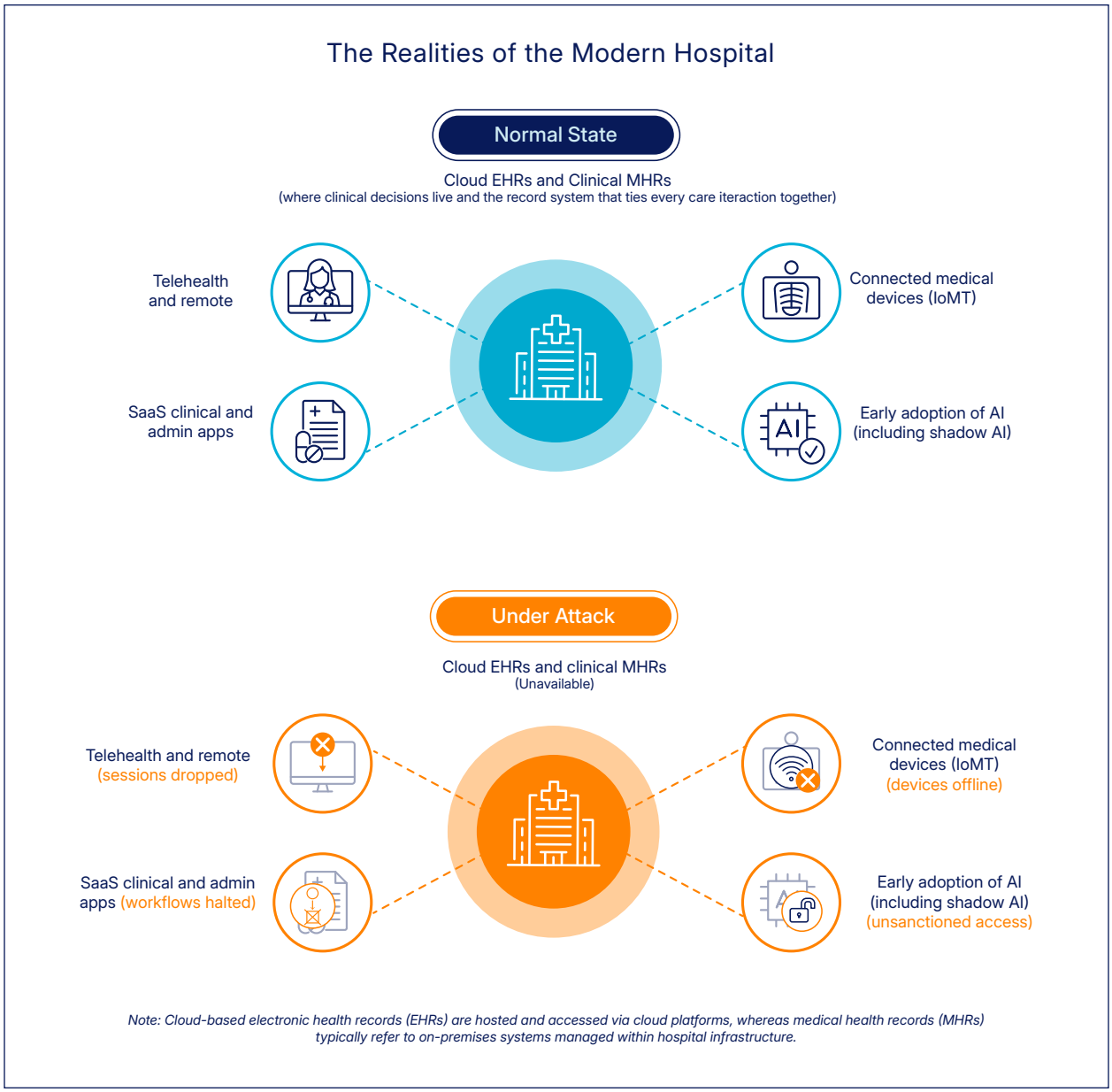
The WannaCry ransomware incident in 2017 had a huge impact on the UK's National Health Service, affecting 80 hospital trusts, forcing the cancellation of nearly 20,000 appointments, and diverting ambulances. More recent incidents such as the Change Healthcare breach affected nearly 190 million people. The CareCloud compromise exposed sensitive patient medical records, and the Stryker attack disrupted medical device management systems.

In recognition of the uniquely sensitive data challenges faced by healthcare organizations, they are required to comply with stringent regulatory frameworks including HIPAA and evolving NIST cybersecurity guidelines , which mandate stronger-than-average controls around data protection, access, and risk management. These requirements have been built with a clear view of the threats. But they do not change the fact that cyber risk in healthcare is persistent, and escalating in both scale and operational impact. As healthcare becomes increasingly digital and AI-enabled, the consequences of future cyber incidents will only become more severe.

Robust data protection is essential to patient safety and to ensure the smooth running of healthcare procedures. Hospital IT leaders must protect multi-layered tech stacks, legacy systems, and vast numbers of users while simultaneously delivering positive patient experiences, driving cost savings, simplifying IT security and networking, and ensuring robust data protection. This is where a modern, zero trust approach to cybersecurity becomes a necessity for today's hospitals.

$9.77m
– the average cost of a data breach in the healthcare sector.

[1] https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf
[2] https://www.reuters.com/business/hack-unitedhealths-tech-unit-impacted-1927-million-people-us-health-dept-website-2025-08-14/
[3] https://techcrunch.com/2026/03/31/carecloud-breach-hackers-accessed-patients-medical-records-ehr/
[4] https://www.cybersecuritydive.com/news/stryker-attack-device-management-microsoft-iran/814816/
[5] https://www.hhs.gov/hipaa/index.html
[6] https://www.nist.gov/cyberframework
[7] https://www.techtarget.com/healthtechsecurity/news/366599336/Average-cost-of-a-healthcare-data-breach-sits-at-977M



Adapting to the modern healthcare frontier

There was a time when healthcare organizations had a single data center located on the premises, which acted as the enforcement point for network security. When staff did occasionally require digital access while working off-site, they were asked to use virtual private networks (VPNs) to connect to the corporate network.

But today's users and applications are everywhere. Remote work is now commonplace, and in healthcare that means collaboration between hospitals, surgeries, laboratories, and community settings. Organizations use dozens of web- and cloud-based applications and operate thousands of interconnected "internet of medical things" (IoMT) devices. This expanded attack surface creates numerous vulnerabilities for adversaries to exploit.

All of this means the traditional perimeter-centric security model built on the presumption that threats only come from outside the network—and that everything inside can be trusted—is no longer adequate. Shifting to a layered defense, designed to protect critical boundaries (particularly where internal systems intersect with external, and often public, networks and resources), is a more effective approach. Legacy point solutions do not share sufficient context across users, devices, apps, and data to ensure everything stays secure and access flows smoothly.

A zero trust approach

Modern security problems demand **a zero trust approach: A comprehensive model built on the principle that no user, device, or system should be trusted by default, regardless of whether they operate inside or outside the network.**

The zero trust philosophy of "never trust, always verify" means, for example, that a physician logging into the electronic health record (EHR) system must prove their identity and authorization, not just once at the beginning of their shift, but throughout as they move between different patient records and clinical apps. This process needn't be laborious, complex, or time-consuming: more on that later.

Zero trust also limits access to the minimum required to perform a specific function—a concept known as least-privilege access. A nurse on the cardiology ward, for instance, would be given access only to the patient records relevant to their current assignment, rather than gaining broad access based on a single login.

These principles reflect the reality that access needs are contextual and constantly changing. This is especially important for hospitals, managing thousands of users across departments, locations, and access levels, from full-time doctors and nurses, to temporary contractors, and from IoMT devices to third-party apps. **Zero trust security provides the granular control and continuous oversight necessary to protect hospitals against both external attacks and insider threats.**

The imperatives of zero trust

Adopting zero trust in healthcare environments requires a structured approach built around three core imperatives: managing risk, ensuring compliance, and safeguarding continuity.

- **Managing risk:** Hospitals face an evolving threat landscape where vulnerabilities can arise from multiple directions, be they sophisticated ransomware attacks, compromised medical devices, phishing attempts targeting clinical staff, or inadvertent data exposure.

  To handle these risks well, security leaders need new capabilities appropriate to the scale of the challenge. Legacy VPNs should be replaced with zero trust network access (ZTNA), and advanced data loss prevention (DLP) and cloud access security broker (CASB) capabilities. Through solutions such as Netskope's patented Zero Trust Engine, hospitals benefit from AI-powered visibility and protection that decrypts and decodes all web, cloud, and private application traffic.

- **Ensuring compliance:** Healthcare organizations operate under some of the most rigorous data protection regulations in any industry, including HIPAA in the United States, GDPR in the Europe Union, and numerous other national and regional requirements for looking after patient information and other data.

  Netskope One provides audit trails to support stringent reporting requirements and ensures consistent policy enforcement. As AI infiltrates healthcare contexts, Netskope's model can also enable the safe use of large language models (LLMs, both private and third party), managing the risk of shadow AI and protecting sensitive prompts.

- **Safeguarding continuity:** Perhaps the most critical concern in healthcare settings is to make sure that security issues never affect the delivery of patient care. Unlike other industries where systems can be taken offline for maintenance or where access delays cause limited inconvenience, hospitals require availability around the clock, while doctors and nurses need instant access to patient information during emergencies

  Netskope's NewEdge Network, the largest private security cloud, ensures resilient network and service availability, eliminating performance trade-offs and ensuring ultra-fast, secure access and experience for clinicians from anywhere in the world.

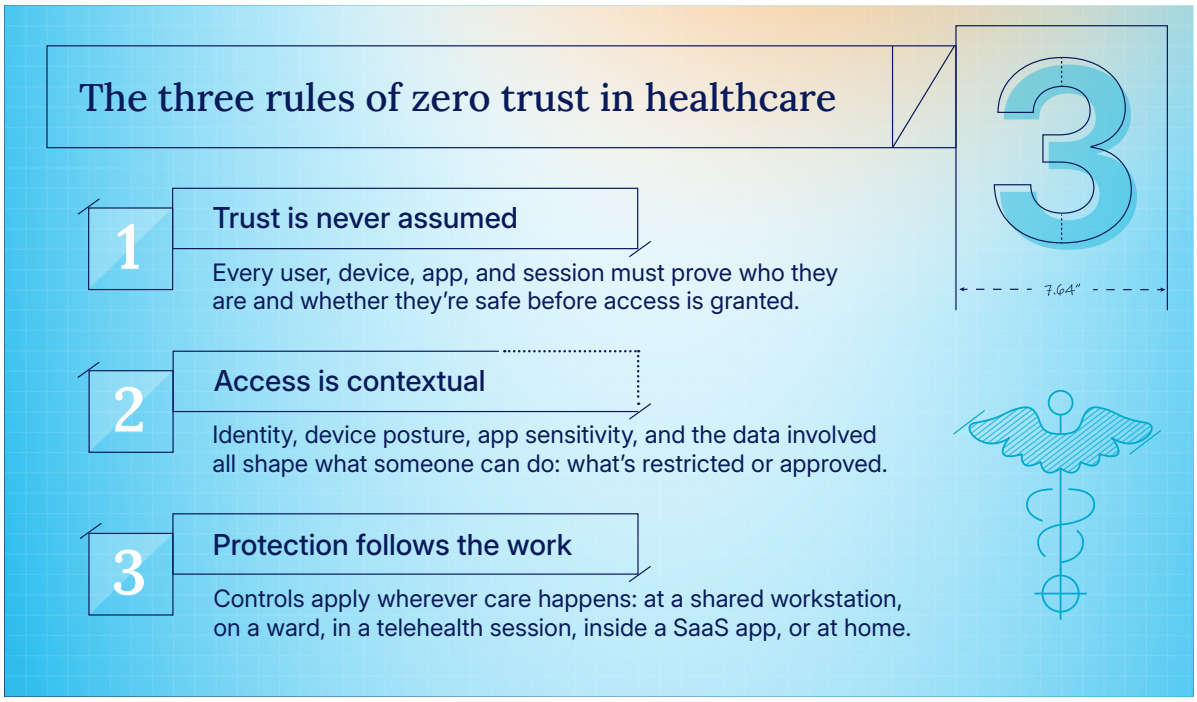
A zero trust hospital framework must be built on these three foundations if it's to effectively protect patient data and ensure uninterrupted clinical operations.

A security architecture built on the principles of zero trust enables a hospital to deliver safe, fast care in modern environments where everything and everyone is connected. Zero trust is a security philosophy that draws on signals from multiple sources within the digital environment. And because of that complexity, it also requires vendors and systems to integrate and provide comprehensive, real-time security.

The architecture of trust

The modern incarnation of zero trust depends on a new set of solutions with capabilities designed to manage the pervasive threats (insider threat, shadow AI, data leakage, and exfiltration) in modern enterprise settings:

Netskope delivers these capabilities through the Netskope One platform, a cloud-native platform that converges security and networking services to help healthcare organizations accelerate their SASE and zero trust transformation.



SASE and SSE:

Secure access service edge (SASE) is a cloud-based framework that integrates wide area networking (WAN) capabilities with comprehensive security services. Security service edge (SSE) is the evolving security stack of tools needed to successfully achieve a SASE architecture. Crucially, SASE enhances visibility and control of the network, allowing security teams to decrypt and decode all traffic for continuous monitoring.

Netskope One provides a unified SASE and SSE architecture that converges networking and security services into a single cloud-native platform. By integrating secure connectivity with advanced security inspection, Netskope enables healthcare organizations to securely support distributed clinicians, remote access, cloud applications, and third-party ecosystems without sacrificing visibility or performance.

DLP:

Data loss prevention (DLP) is a set of cloud-native strategies and tools designed to prevent sensitive information from being lost, stolen, or accessed by unauthorized users. Advanced, AI-powered DLP tools are vital in preventing the exfiltration of PHI and personally identifiable information (PII).

Netskope One delivers AI-powered, DLP capabilities designed to protect sensitive healthcare data across cloud services, web traffic, private applications, email, endpoints, and AI applications.

CASB and SWG:

These solutions protect data at rest and in motion across managed and unmanaged cloud and web apps. Cloud access security brokers (CASBs) sit between users and cloud service providers to enforce security policies and provide visibility into cloud usage. Secure web gateways (SWGs) protect users from web-based threats, effectively serving as an inspection point between users and the internet to prevent malware infections and data breaches.

Netskope One's advanced CASB and SWG capabilities deliver visibility, adaptive policy enforcement, and data protection across managed and unmanaged cloud applications and services.

DSPM:

Data security posture management (DSPM) is an advanced approach that automatically discovers, classifies, and monitors sensitive data across cloud environments. This gives organizations visibility into where their critical data resides, who has access to it, and how it's being used. DSPM provides deep visibility into data that often lies outside the traditional sphere of IT control.

Netskope advocates for a unified approach that combines the discovery and governance capabilities of DSPM with the real-time protection of DLP, to help healthcare organizations discover, classify, and monitor sensitive data across cloud and hybrid environments.

Signals from across the digital ecosystem

Zero trust is a story of integration, combining signals from multiple sources within a hospital's digital ecosystem. The key to an effective zero trust approach is to share, correlate, and operationalize these signals, ensuring they are not trapped inside individual point solutions.

Consistently interpreting these signals means applying a unified understanding of risk across users, devices, applications, networks, and data, so that security decisions remain coordinated, context-aware, and continuously adaptive as conditions change throughout a clinical workflow.

Importantly, zero trust is not a one-time authentication decision. Trust must be continually evaluated and adapted based on changing context, including user behavior, device posture, application activity, network location, and data sensitivity.

- **Access and identities:** clinicians, support staff, contractors, vendors, and non-human identities.

  A wide variety of users access hospital systems, and each user type has unique access requirements and risk profiles that must be evaluated in real time. In fast-paced clinical environments, for example, touch-and-go access models allow clinicians to move seamlessly between devices and locations while maintaining secure, authenticated access. By aggregating identity signals across these categories, hospitals can enforce least-privilege access principles, determine policy for AI agents (non-human identities), and more easily detect anomalous behavior that might indicate compromised credentials or insider threats.

- **Devices and IoMT:** laptops, tablets, scanners, pumps, imaging and lab equipment.

  Modern hospital environments include thousands of connected devices, ranging from traditional IT endpoints such as laptops and tablets to specialized IoMT devices. Collecting and analyzing signals from this diverse ecosystem helps security teams better detect vulnerabilities and prevent compromised devices from accessing clinical networks.

- **Apps and workloads:** EHR, SaaS, on-premises clinical systems.

  Healthcare applications span a complex landscape, from mission-critical EHR systems to cloud-based SaaS platforms and legacy on-premises clinical apps. Each one generates valuable information about user behavior, data access patterns, and potential security events that contribute to the overall threat picture.

- **Networks and connectivity:** on-site, remote, and roaming users.

  Hospital networks must handle users connecting from multiple locations and contexts, including main campuses, satellite clinics, home offices, and mobile devices used by staff on the move. Network signals provide crucial context about user location, connection security, and whether traffic patterns align with expected behavior. These help organizations to enforce location-based access policies and ensure consistent security, regardless of where care is being delivered.

Organizations can safely enable the use of AI by applying real-time guardrails. Netskope identifies when sensitive patient data or proprietary research is being pasted into public AI prompts and can automatically redact the information or block the activity, preventing data leakage into public training sets. Netskope ensures that as data is shared with third-party partners (for example, research teams) or moved into analytics platforms, it remains wrapped in a zero trust policy that follows the data itself, regardless of where it is stored or processed.

- **Data and AI:** PHI, clinical images, documents, prompts, logs.

  The crown jewels of healthcare organizations include PHI, diagnostic images such as X-rays and scans, clinical notes, and increasingly, the prompts and outputs from AI systems used for support in decision-making. System logs and audit trails are critical in revealing security incidents or compliance violations. Monitoring how this sensitive data is accessed, moved, and used across the organization provides essential signals for detecting data exfiltration attempts, identifying risks from shadow IT, or ensuring that privacy regulations are being followed.

Why the ecosystem matters

Healthcare security is an ecosystem, not a monolith. There's no single tool that makes a hospital zero trust-ready. Instead, an effective zero trust model requires shared context across identity, device posture, segmentation, data protection, and recovery, to deliver real safety and resilience.

This is where an ecosystem of technologies plays a crucial role, with each technology providing essential inputs into robust security processes. Netskope works with industry-leading partners across multiple domains to provide a thorough approach, together creating the real-time intelligence that zero trust depends on.

Identity and access

Identity is foundational to zero trust in healthcare environments, where clinicians require fast, seamless, and secure access to systems containing sensitive patient information. Integrations across identity, privileged access, and authentication platforms help healthcare organizations enforce adaptive, identity-aware access controls while maintaining efficient clinical workflows, including support for shared workstations, roaming clinicians, and privileged administrative access.

Integrations include: Imprivata, Microsoft Entra, CyberArk

Endpoint and device posture

Healthcare organizations must secure a diverse and constantly changing endpoint landscape that includes clinical workstations, thin clients, unmanaged devices, and internet of medical things (IoMT) equipment. Integrations with endpoint protection, XDR, device management, and asset visibility platforms provide real-time posture assessment and threat intelligence that can be used to dynamically enforce zero trust policies and contain threats before they spread across the clinical environment.

Integrations include: CrowdStrike, SentinelOne, IGEL, Forescout

Containment and segmentation

Segmentation and containment technologies help healthcare organizations limit lateral movement and reduce the impact of ransomware or compromised workloads. By sharing risk intelligence and workload context between platforms, organizations can automatically isolate affected systems, restrict access, and continuously adapt security policies based on changing risk conditions across hybrid environments.

Integrations include: Illumio, ColorTokens

Recovery and resilience

Cyber resilience requires healthcare organizations to rapidly recover critical systems and sensitive patient data following a cyber incident. Integrations across backup, recovery, and data security platforms help organizations prioritize the restoration of high-value clinical data, validate backup integrity, and reduce the risk of reinfection while supporting compliance with healthcare and regulatory requirements.

Integrations include: Rubrik, Commvault

IT workflows and response

Healthcare security operations rely on coordinated workflows across IT, security, and compliance teams. Integrations with IT service management (ITSM), security orchestration, automation, and response (SOAR), and security information and event management (SIEM) platforms enable organizations to automate incident response, improve operational efficiency, accelerate investigations, and maintain consistent policy-driven remediation processes across the healthcare environment.

Integrations include: ServiceNow, Tines, Splunk

Core clinical platforms

Clinical applications and electronic health record (EHR) platforms contain some of the most sensitive data in healthcare environments. Integrations with core clinical systems help healthcare organizations apply consistent zero trust controls around access, data movement, and user activity while preserving the performance and usability required for patient care delivery across hospitals, clinics, and telehealth environments.

Integrations include: Epic, Cerner

3. A day in the life of a zero trust hospital: Room-by-room

The best way to understand the ongoing benefits of the zero trust hospital is to follow a single clinician through their daily work.

Meet Sam, a nurse starting an early shift. As they move from room to room, Sam faces a familiar set of workflows, each one essential to patient care but each carrying its own cyber risk. Thankfully, zero trust architecture is here to protect Sam's patients' private data.

3.1. Start of the journey: Shared workstation

Scenario:

Sam arrives on the ward, taps into a shared workstation, and logs in to check assignments and patient notes.

Risk:

Shared devices create opportunities for session hijacking, over-privileged access, and accidental exposure of PHI.

What happens:

Netskope ZTNA/SWG applies context-aware access and continuous session controls. DLP maintains audit trails and blocks high-risk actions relating to patient data.

Partner Integration:

Fast, verified login is enabled through Imprivata or Microsoft Entra. Endpoint posture signals taken from CrowdStrike or SentinelOne confirm the device is safe.

Outcome:

Sam gets rapid access without friction, but only in the right context, with every session tracked.

3.2. Moving between clinical apps and SaaS

Scenario:

Sam moves across rooms, accessing EHR, imaging, scheduling, and SaaS tools.

Risk:

Inconsistent controls across apps cause security gaps for data leakage or unauthorized access. Proliferation of unmanaged SaaS tools leads to PHI entering apps that lack proper encryption and controls.

What happens:

Netskope's SSE enforces unified policies regardless of the app being used. CASB identifies shadow IT tools and manages or blocks them.

Partner Integration:

If Sam interacts with core clinical platforms like Epic or Cerner, Netskope's Zero Trust Engine works alongside these partners to apply granular, real-time DLP policies. This ensures that sensitive PHI is protected even when transitioning between local clinical workloads and web-based SaaS tools, preventing data leakage into unmanaged shadow IT applications that may have been identified by Netskope's CASB.

Outcome:

Sam can move seamlessly without delays, keeping patient care running smoothly, while security teams have confidence that consistent policies are enforced everywhere.

3.3. Telehealth and remote care touchpoint

Scenario:

Sam supports a virtual consultation with a remote clinician.

Risk:

Dramatic expansion of the hospital's attack surface. Staff connect from unmanaged endpoints and accidentally enable malware or other unsafe access into clinical systems.

What happens:

Netskope's ZTNA principles grants least-privilege access to the remote clinician. DLP inspects all traffic in real time, while CASB/SWG functionality provides visibility into which tools the remote clinician is using.

7.64"

Partner Integration:

Netskope integrates with Okta or Microsoft Entra to enforce continuous, risk-based identity verification, ensuring that the remote clinician supporting Sam is securely authenticated before accessing telehealth systems. In parallel, integrations with endpoint security partners such as CrowdStrike or SentinelOne assess device posture in real time. If the clinician's unmanaged device is deemed high risk, Netskope can automatically initiate remote browser isolation (RBI), enabling them to securely interact with clinical applications and collaborate with Sam without exposing the hospital network to potential threats.

Outcome:

Both Sam and the remote clinician enjoy secure collaboration without compromise—fast, efficient, and frustration-free.

3.4. Remote radiology and specialist access

Scenario:

Sam asks for an image read from a radiologist working remotely, requiring the radiologist to access the hospital's image system.

Risk:

Traditional VPN architectures force traffic to backhaul through the hospital's data center, creating performance bottlenecks and granting overly broad access to systems.

What happens:

SSE architecture provides the remote radiologist with direct, optimized connectivity to key systems. The radiologist's device, location, behavior patterns, and data being accessed are continuously assessed, with dynamic security controls applied.

Partner Integration:

Netskope integrates with Microsoft Entra or Okta to provide the remote radiologist supporting Sam with seamless, identity-aware access, eliminating the need for traditional VPNs and reducing latency. At the same time, integrations with endpoint security partners such as CrowdStrike or SentinelOne ensure that the radiologist's device is continuously assessed for compliance and threats before any imaging data is accessed or shared with Sam.

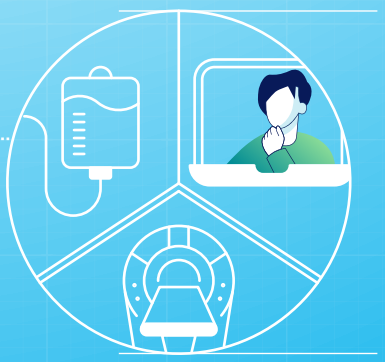
Outcome:

Information flows between Sam and the radiologist without delays, providing a better experience for them, faster answers for patients, and comprehensive audit trails for IT.

3.5. IoMT and a device-heavy ward

Scenario:

Sam works on the ward, switching between key equipment such as pumps, monitors, scanners, and diagnostic devices.



Risk:

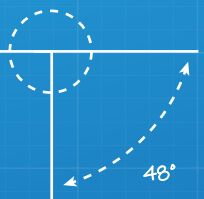
Flat network architectures mean devices share the same network segment as traditional IT systems, creating pathways for attackers to gain access through unmanaged IoMT, move laterally, and spread ransomware.

What happens:

With granular segmentation, the Netskope architecture isolates IoMT devices from general IT networks and from each other, based on device type, function, and risk profile. Constant monitoring of network traffic to detect anomalies.

Partner Integration:

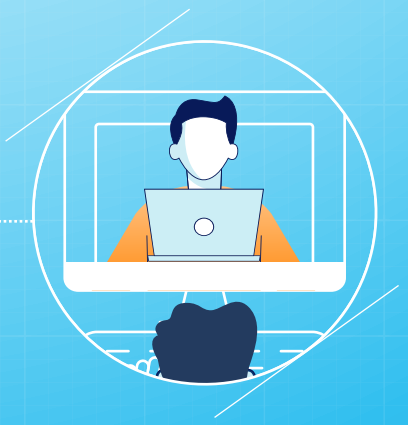
Netskope integrates with Forescout to eliminate visibility gaps across IoMT environments, combining deep device discovery with the Netskope One Gateway to identify the make, model, and clinical function of every device Sam interacts with on the ward. In parallel, integration with endpoint security partners such as CrowdStrike or SentinelOne ensures that the workstations Sam uses are continuously monitored and protected, preventing compromised endpoints from enabling lateral movement into the IoMT network.



Outcome:

Medical devices operate more reliably, with stronger protection leading to better patient care and improved device uptime.

3.6. Vendor and third-party access



Scenario:

The hospital's EHR system experiences software problems, so a vendor connects in to troubleshoot and provide technical support.

Risk:

Third parties receive overly broad access privileges, allowing them to view sensitive patient data or access unrelated systems. Vendor sessions are poorly monitored, enabling external compromise and creating a pathway for internal risk and lateral movement.

What happens:

Temporary, just-in-time access policies ensure that the vendor is only connected for a specific maintenance window, with access revoked immediately afterward. Netskope provides detailed logging and session recording, eliminating blind spot.

Partner Integration:

Netskope integrates with Imprivata, Microsoft Entra, and Okta to enforce stringent, identity-centric controls over third-party access, ensuring that any vendor supporting Sam's systems is authenticated and granted only the minimum required privileges. Integration with ServiceNow and Splunk ensures that every vendor action is fully documented and auditable. ServiceNow automates approval workflows for temporary access requests, while Splunk ingests Netskope's detailed activity logs to provide real-time monitoring of each session.

Outcome:

Sam and other clinical staff experience minimal disruption as the vendor quickly resolves the performance issue, while the security team's operational needs and compliance requirements are satisfied.

3.7. Everyday SaaS and AI use

Scenario:

Sam uses an AI tool to summarize extensive notes and draft patient-friendly language for sensitive communications.

Risk:

PHI gets uploaded into unmanaged AI tools and sensitive files synced to personal clouds, compromising patient confidentiality and creating serious compliance violations. Shadow IT tools operate without security approval or configuration.

7.64"

What happens:

Granular visibility policies identify all tools in use and can block sensitive uploads. Through advanced DLP, Netskope scans AI prompts in real time to detect PHI and block it where appropriate. All prompts are logged for future auditing.

Partner Integration:

Netskope integrates with Microsoft Entra and Okta to ensure that Sam only accesses AI and SaaS platforms through a verified, identity-aware framework powered by the Netskope Zero Trust Engine. By combining these identity controls with Netskope's Cloud Confidence Index (CCI), healthcare organizations can dynamically evaluate the risk of over 85,000 SaaS apps, AI applications, and public Model Context Protocol (MCP) servers. As a foundational capability of Netskope One AI Security, this empowers teams to automate access decisions, enabling seamless single sign-on (SSO) into trusted managed AI tools, while restricting or limiting interactions with higher-risk, unmanaged AI applications.

Outcome:

Using an approved, compliant tool, Sam saves time and improves care quality without comprising the healthcare environment.

3.8. Incident response and clean recovery

Scenario:

As Sam's shift comes to an end, suspicious activity disrupts clinical systems.

Risk:

Compromised systems lead to extended downtime as security teams struggle to contain the issue and determine its full impact. Delayed recovery forces staff to revert to paper documents and manual tracking, affecting patient care.

What happens:

With real-time insight across the entire digital ecosystem, Netskope's SSE provides rapid understanding of the incident scope. Compromised users, devices, and applications are quarantined upon detection.

Partner Integration:

Netskope integrates with ServiceNow and Tines to trigger automated response workflows, ensuring that incidents impacting Sam's environment are rapidly contained and escalated to the appropriate teams. At the same time, integration with data resilience platforms such as Rubrik or Commvault enables identification of the last known clean state of affected systems. This allows security teams to precisely scope the incident and initiate a targeted, rapid recovery of clinical operations.

564

Outcome:

Patient care continues as the security team quickly identifies and contains the issue.

4. FROM BLUEPRINT TO BUILD: WHERE LEADERS START

With hospitals' digital environments under more strain than ever, legacy security approaches are no longer fit for purpose. There's an urgent need for healthcare leaders to transition to a model where no user, device, or application is inherently trusted: the zero trust philosophy.

That's a mindset shift as well as a technical upgrade. But moving to a more robust zero trust security architecture shouldn't be overwhelming. In this section, we outline a four-step roadmap to getting started that builds momentum and executive support pragmatically.

Getting started with zero trust

The benefits of zero trust are evident—the question for hospital CISOs and CIOs is how to adopt it. The struggle is to translate the high-level principles of zero trust into straightforward and practical steps, particularly in environments constrained by legacy systems, limited budgets, and risk-averse cultures.

The most effective path forward is incremental: a phased and pragmatic approach that delivers early wins to demonstrate the value of zero trust, builds confidence, and expands protections over time. The following four phases offer a practical roadmap for adoption, prioritizing the most critical risks first and creating a foundation for sustained resilience.

Phase 1 – Fix access

Start by replacing painful VPN access with ZTNA and clean identity integration.

Goal: fast, safe access for staff and partners

The foundation of any zero trust transformation is modernizing how users connect to hospital systems and applications. By replacing legacy VPN infrastructure with ZTNA solutions, hospitals can stop granting network-level access and create direct, encrypted connections between verified users and specific applications. A remote physician accessing an EHR system, for instance, never sees billing details, research databases, or other unrelated resources.

The result is an improved user experience, with single sign-on (SSO) and seamless application access, alongside stronger security that prevents lateral movement during breaches. For hospitals supporting distributed workforces, contractors, and third-party partners, this identity-centric approach establishes the access controls that underpin all subsequent zero trust capabilities.

Phase 2 – Protect data wherever it goes

Extend lightweight controls across web, SaaS, and emerging AI use.

Goal: stop accidental PHI exposure without slowing people down

Once identity and access controls are in place, focus can shift to protecting patient data as it moves beyond the hospital perimeter into cloud applications, web-based tools, and across the entire AI ecosystem. To secure both human users and non-human agentic workflows, hospitals need the Netskope One AI Gateway

and Netskope One Agentic Broker, alongside Netskope One NG-SWG and CASB. Together, these provide inline inspection and control of data flows—whether from a user prompt or an autonomous app-to-LLM API call—without adding latency or disrupting clinical workflows. Adding Netskope One AI Guardrails enables the enforcement of semantic DLP, evaluating the actual meaning of content and preventing accidental exposure of protected PHI.

As organizations increasingly experiment with AI for clinical summaries, diagnostics, and automation, this active defense layer becomes critical. Controls must detect attempts to submit PHI to external AI services. The Netskope One platform uses real-time "coach and pivot" alerts to safely guide users toward managed AI alternatives, or redacts sensitive data before transmission. By emphasizing transparency and minimal friction, hospitals can protect patient privacy without slowing staff down or driving them toward risky, unmanaged IT and AI applications.

Phase 3 – Bring devices and vendors into view

Fold IoMT, medical equipment, and third-party access into the same model.

Goal: reduce blind spots and shrink lateral movement

With identity-based access and data protection in place, hospitals can then extend zero trust to the sprawling ecosystem of medical devices, IoMT equipment, and third-party connections that often cause major security blind spots. Unlike traditional IT assets, many medical devices run unpatchable operating systems, lack modern authentication, and were never designed with security in mind.

This phase focuses on device visibility and network segmentation to identify every connected asset, understand normal communication patterns, and isolate devices into microsegmented zones that prevent compromised assets from becoming attack launch points. By bringing devices and external partners into the same identity-driven, continuously verified framework as staff, hospitals sharply reduce their attack surface and eliminate the lateral movement paths that ransomware relies on.

Phase 4 – Strengthen response and recovery

Tighten telemetry, containment, and clean restore with SIEM/SOAR/XDR and backup partners.

Goal: recover quickly and confidently when something goes wrong

The final phase recognizes that no architecture is invincible. This makes rapid detection, containment, and recovery essential to hospital resilience. The focus is on unifying the telemetry established earlier: identity events, access decisions, device and user behaviour, and data movement can then be fed into security information and event management (SIEM), security orchestration and response (SOAR), and extended detection and response (XDR) platforms that can correlate signals and automate workflows across the environment to surface advanced threats.

Analytics helps identify subtle indicators of compromise, such as anomalous logins or unusual data access patterns. When threats are detected, automated response playbooks can quickly limit impact by isolating systems, revoking credentials, blocking malicious traffic, and alerting security teams, while preserving forensic evidence. The objective is organizational resilience, providing confidence that when incidents inevitably occur, the hospital can detect them quickly, contain damage, restore operations, and strengthen defenses for the future.

The zero trust imperative

Adopting a zero trust security approach helps hospitals align security, risk, compliance, and operational continuity around a single, coherent framework. Instead of treating these as competing priorities, zero trust embeds protection, access governance, and visibility in ways that support regulatory requirements, risk management, and uninterrupted clinical operations at the same time.

Zero trust dramatically reduces friction in clinicians' daily work by making secure access simpler, faster, and more consistent. Clinicians can access records, applications, and collaboration tools from any location without delay, while security controls protect patient data invisibly. The result is a security posture that clinicians actually embrace rather than circumvent, because it makes their work easier.

The transition to zero trust is no longer optional for hospitals that take their security obligations seriously. So whether your hospital is just beginning to explore zero trust concepts, or you're ready to accelerate an existing transformation, the time to act is now. Contact us today to book a demo and discover how Netskope's zero trust solutions can be tailored to your specific clinical workflows, regulatory requirements, and security challenges. Take the first step toward a future where robust security enables rather than impedes exceptional patient care.

Take the Zero Trust Maturity Assessment Now

Interested in learning more?

Request a demo

Netskope, a leader in modern security and networking, addresses the needs of both security and networking teams by providing optimized access and real-time, context-based security for people, devices, and data anywhere they go. Thousands of customers, including more than 30 of the Fortune 100, trust the Netskope One platform, its Zero Trust Engine, and its powerful NewEdge network to reduce risk and gain full visibility and control over cloud, AI, SaaS, web, and private applications—providing security and accelerating performance without trade-offs.