Designing for Continuous Compliance in Healthcare

Five ways zero trust and SASE make continuous compliance a reality for healthcare.

netskope

Table of Contents

Continuous compliance is now a patient safety issue

The link between patient safety and compliance is becoming increasingly clear, and it's being shaped by a convergence of opportunities, challenges, and threats that the healthcare industry has been navigating for some time now.

Modern care now depends on a dense digital stack of EHRs, cloud-based clinical apps, telehealth, connected devices, and AI-assisted tools. These systems save clinicians time, support more targeted treatments, and improve overall continuity of care.

But at the same time, the threat landscape has intensified, with healthcare routinely among the most targeted sectors for ransomware and double-extortion campaigns. These attacks are designed to disrupt care, not just steal data.

A single compromised tool can freeze claims, delay prescriptions, and force staff back to manual workarounds, with real consequences for patients' access to timely treatment.

The combination of aggressive cyber adversaries, accelerating digital transformation, and tougher regulations has made compliance controls as critical as staffing levels, bed availability, and clinical workflows.

That's why continuous compliance is now directly tied to patient safety. Healthcare leaders need operating models that maintain visibility, control, and assurance every day across every application, device, and data flow that care depends on.

When risk, compliance and continuity are aligned, patient care sits at the centre.

Why traditional approaches can’t keep up

While most healthcare organizations can quote the regulations, the ability to prove at any moment that controls are working everywhere patient data flows is where traditional compliance approaches begin to falter.

Many environments still run on aging networks with VPNs bolted on, and a patchwork of separate tools for data protection, email, AI use, and connected devices. Each tool solves a narrow problem, but together they create policy silos, blind spots, and duplicated effort—too many point solutions and not enough control or visibility.

Over time, this leaves healthcare institutions with fragmented control environments where no one has a single, trusted view of where protected health information (PHI) is going or which controls actually apply.

This results in a number of issues for traditional healthcare organizations:

Spreadsheet compliance doesn’t scale

For many institutions, proving control coverage remains a painfully manual process. Teams spend weeks chasing screenshots, exports, and logs, then trying to map them against HIPAA, NIS2, or internal policies. This results in too much time, energy, and budget being spent documenting yesterday instead of strengthening the present.

Care and data are now truly everywhere

Clinicians, third parties, remote coders, and billing partners all access critical apps and PHI from different locations, devices, and networks. Add in hard-to-patch Internet of Medical Things (IoMT) devices and legacy clinical systems, and the old idea of “trusting the network perimeter” has lost all meaning.

AI opens a new attack and compliance surface

More PHI and intellectual property now drift into the public cloud as “shadow” AI tools—often used without security teams’ knowledge—become more common. Without consistent, data-centric controls, it’s almost impossible to prove you’re governing this new channel properly.

This multi-pronged pressure can make continuous compliance feel aspirational rather than achievable. But closing the gap between “we know the regs” and “we can prove we’re compliant at any moment” simply requires a different approach—one built on zero trust principles and a secure access service edge (SASE) or security service edge (SSE) architecture with data protection at its core.

This eBook is designed to help healthcare teams navigate the growing complexity of continuous compliance. Achieving this requires more than meeting regulatory checklists—it demands an architectural shift that aligns risk, compliance, and continuity around the realities of zero trust and a modern hospital blueprint. In this eBook, we'll look more closely at how these forces intersect, and what it takes to keep patient care at the center of that equation.

To make this practical, we outline five rules that help organizations build continuous compliance into everyday operations rather than treating it as a periodic exercise. These rules focus on the foundations healthcare teams rely on most:

- Visibility
- Least-privilege access
- Data and AI protection
- Architectural resilience
- Ongoing audit readiness

Throughout, we consider the major regulations and frameworks that shape healthcare security obligations—HIPAA, NIS2, GDPR, the EU AI Act, and NIST CSF—and show how each rule connects to these requirements in real, operational terms.

Finally, we will demonstrate how these five rules align to Netskope's security and networking solutions to support this.

The Netskope One platform brings together the full spectrum of SSE and SASE capabilities within a single, unified platform—including:

- Software-defined Wide Area Networking (SD-WAN)
- Cloud Access Security Broker (CASB)
- Next Gen Secure Web Gateway (Next Gen SWG)
- Universal Zero Trust Network Access (UZTNA)
- Data Security Posture Management (DSPM)
- Data Loss Prevention (DLP)
- Remote Browser Isolation (RBI)
- Enterprise Browser (EB)
- Firewall as a Service (FWaaS)
- Digital Experience Management (DEM)

This convergence delivers the architectural consistency and unified policy enforcement required for continuous compliance. It also provides a clear foundation for mapping SASE controls to healthcare security and regulatory frameworks, helping teams operationalize these five rules across distributed clinical environments.

Rule 1. Start with real-time visibility, not annual audits

Most healthcare compliance still relies on periodic evidence pulls, static screenshots, and manual checks—leaving long gaps where no one can say which controls are active, where PHI is flowing, or whether policies are enforced.

The issue isn't lack of effort—it's that the tools and processes in place were never built for data that moves this fast or this widely.

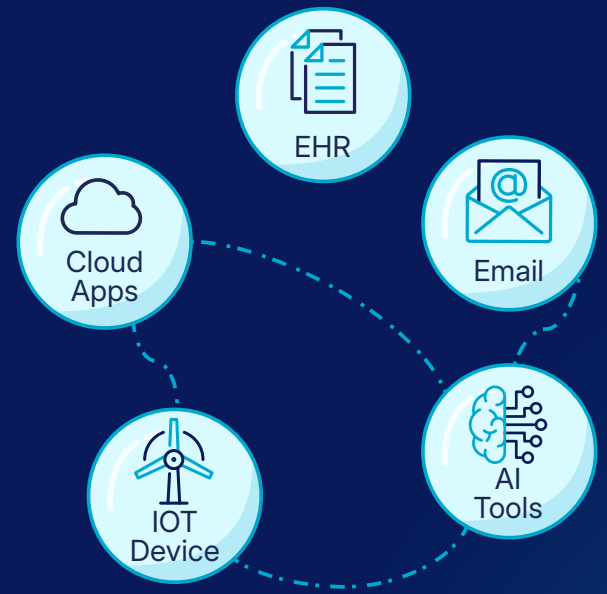
PHI now moves constantly across cloud apps, devices, clinical systems, and AI tools. Without real-time telemetry or unified policies following that movement, even well-run compliance programs end up reactive.

The new imperative

Continuous compliance starts with real-time insights into users, devices, data movement, and control coverage across clinical settings. Instead of reconstructing events weeks later, teams can see violations as they emerge, follow PHI between apps and partners, and validate protections at each access point.

This shifts compliance from a retrospective "prove it later" exercise to an operational reality you can enact in real time.

Legacy approach: Periodic audits and manual evidence pulls



Quarterly Audit Report

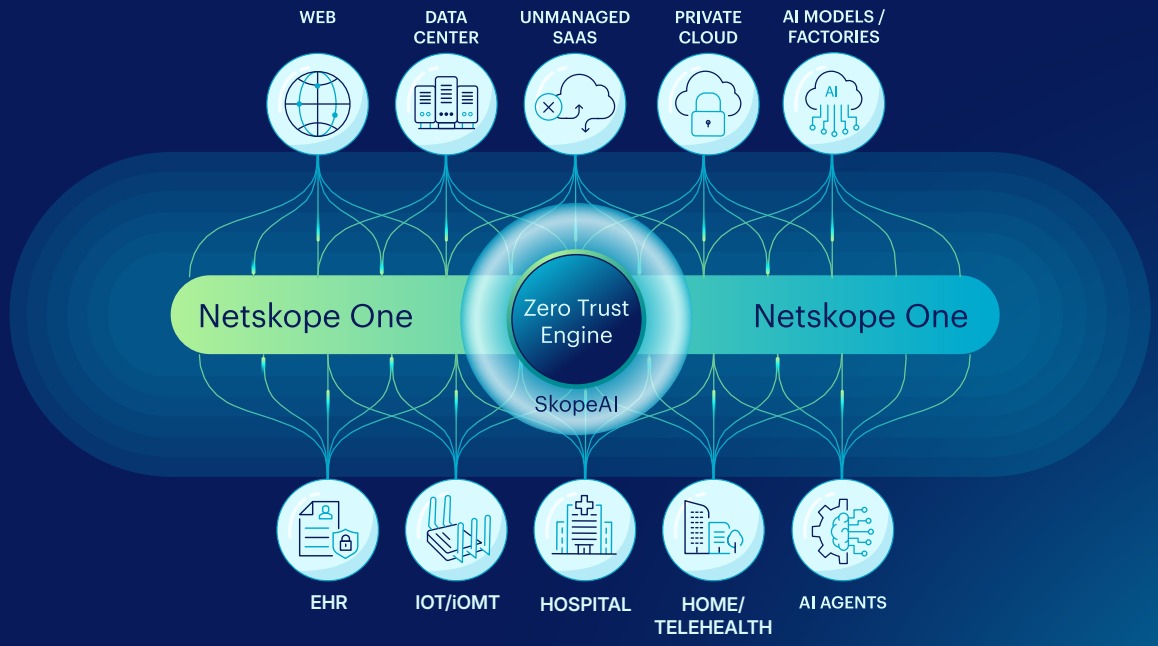
- Static screenshots
- No continuous view
- Long gaps between checks
- Uncertain control coverage

Continuous compliance depends on seeing controls, PHI flows, and risks as they happen, not weeks later. Instead of stitching together screenshots, teams need live, unified telemetry across cloud apps, remote clinics, IoMT devices, and AI tools. Gaps should also surface the moment they appear, with alerts for drift, unusual data flows, or control failures so that issues can be fixed in hours, not discovered months later.

Solution: Netskope One & Advanced Analytics* (HIPAA, NIS2, NIST CSF)

- Netskope One provides unified visibility across web, SaaS, IaaS, and private applications.
- Advanced Analytics provides a real-time view of control coverage and drift.
- Continuous telemetry mapped to HIPAA, NIS2, and NIST CSF creates defensible, automatically generated evidence that replaces periodic audits with continuous assurance.

Modern approach: Real-time, unified, continuous



Footnote:

**Netskope Advanced Analytics helps organizations understand and manage their exposure to cloud risks by providing a 360° view of activity throughout the Netskope One platform.*

Rule 2. Enforce least-privileged access and segmentation everywhere

VPNs that grant broad, network-level access are still common in healthcare, giving clinicians, contractors, and third parties far more access than necessary. Once someone is “on the network,” limiting their movement or proving that access is only granted at minimum-necessary standards becomes difficult.

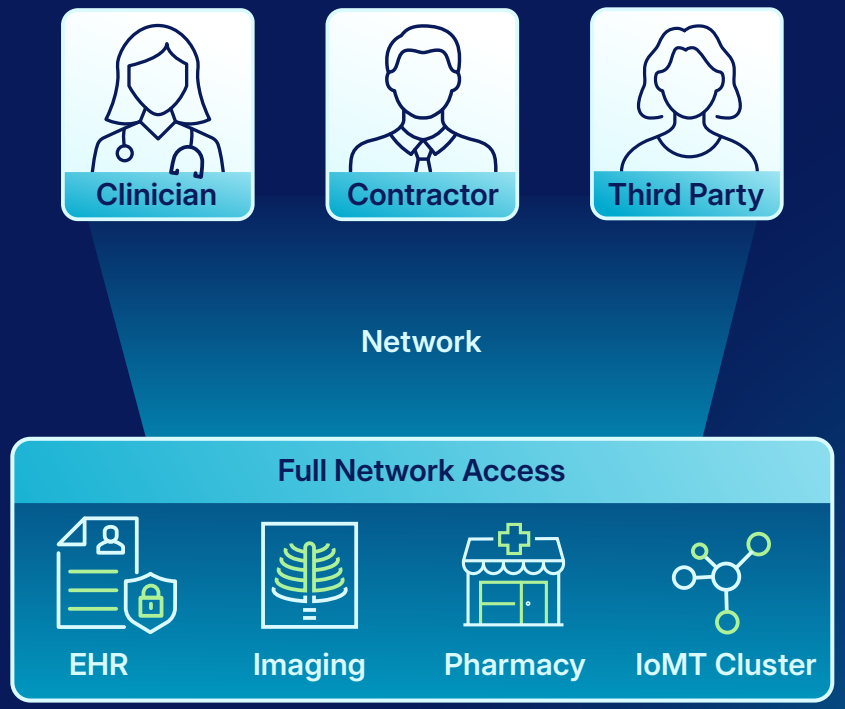
The core issue is a model that bases trust on location rather than risk: If a device sits inside the hospital network or connects via VPN, it’s often trusted by default.

This leaves critical systems and IoMT devices on flat or poorly segmented networks, making lateral movement easy and turning a single weak point into a patient safety or compliance event.

The new imperative

Users should access only the specific apps and data they need. IoMT devices should be visible, profiled, and isolated so they communicate only with required systems. Access should adapt to real-time signals—device posture, behavior, location—shifting control from a binary VPN check to a fine-grained, context-aware policy.

Broad VPN access and flat network exposure



It's important to replace broad VPN access with application-level controls that expose only the clinical and business apps a user needs.

Zero trust segmentation then ensures IoMT and critical systems are on tightly controlled paths so compromised devices can't be used for lateral movement. Access should also adapt to real-time signals—device posture, behavior, and location—triggering step-up verification or access blocks when risk is high.

Solution: Netskope ZTNA & Zero Trust Engine* (HIPAA, GDPR, NIS2, NIST CSF)

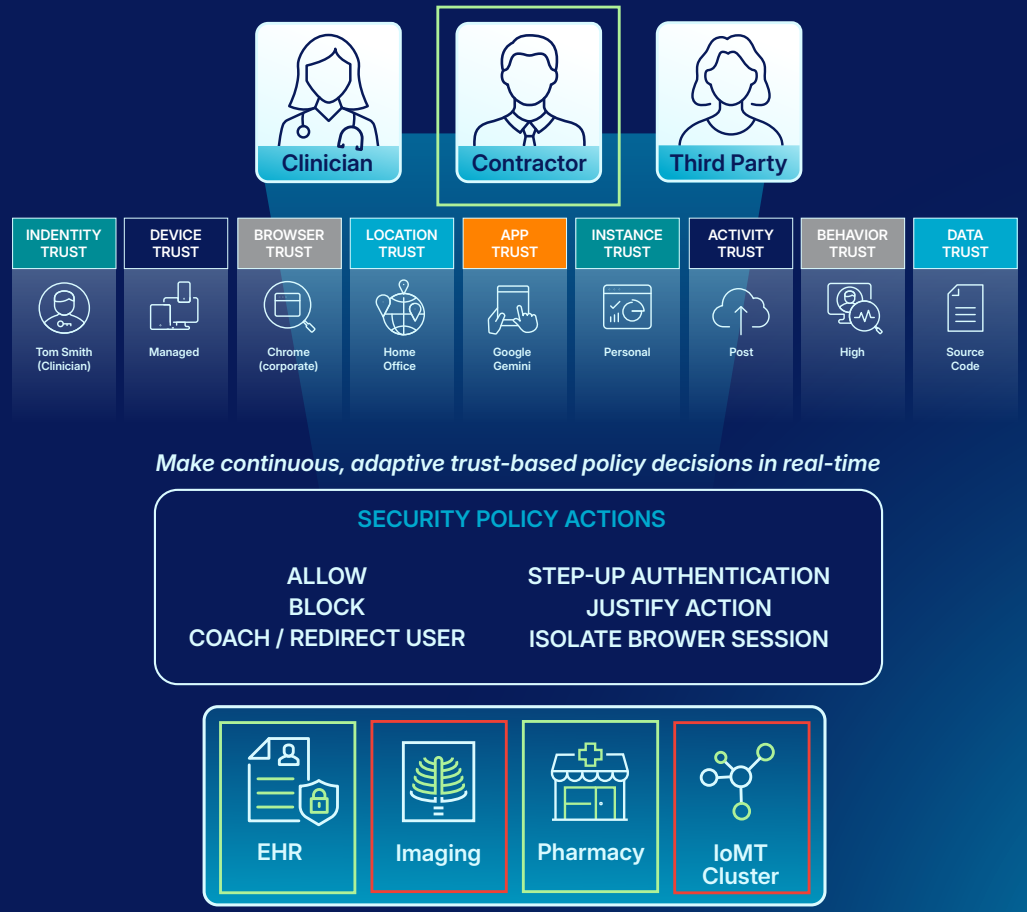
- Netskope ZTNA and the Zero Trust Engine continuously evaluate user, device, app, and data context.
- ZTNA replaces VPN over-privileged access with granular, least-privileged access aligned to HIPAA Minimum Necessary and GDPR requirements.
- Device Intelligence** and segmentation isolate IoMT devices by profiling behaviors and detecting anomalies, reducing lateral movement in line with NIS2 and NIST CSF access control expectations.

Footnote:

**Netskope Zero Trust Engine is a foundational component of the Netskope One platform. It plays a pivotal role in gathering comprehensive risk telemetry and delivering unmatched contextual awareness to enable adaptive, least-privileged access to users, devices, applications, and data.*

***Netskope Device Intelligence provides unprecedented visibility into all connected devices across enterprise networks and branch offices, and secures them through context-driven classification, risk assessment, segmentation, and access control.*

Least-privilege access shaped by role and risk



Rule 3. Make data and AI protection ‘by design’, not bolt-ons

Many healthcare organizations still rely on a patchwork of controls to keep PHI in the right places, leaving them with fragmented systems. Email has one set of rules, cloud storage another, EHR exports another, and generative AI tools often sit outside any governed process.

It only takes an accidental upload, misdirected share, or copy-paste into an AI tool for PHI to slip through the cracks.

The deeper issue is that policies are app-centric, not data-centric. Once PHI leaves a core clinical system, it stops being treated as regulated and becomes “just another file.” No single view or policy follows that data end-to-end. Proving data protection by design becomes impossible when you can’t see or control where PHI travels.

The new imperative

Organizations need a unified way to discover, classify, and protect PHI everywhere. Continuous compliance means inspecting traffic across web, SaaS, IaaS and private apps, applying consistent policies and recognizing PHI by context, not file type.

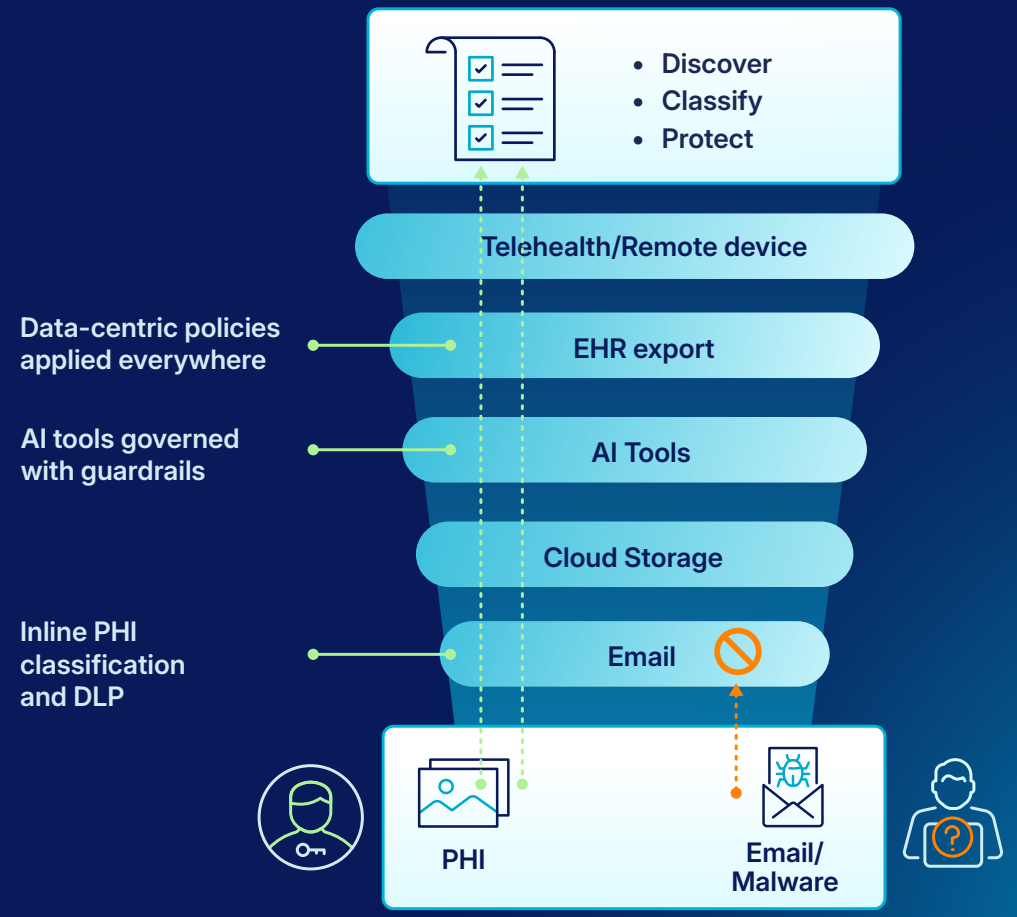
Fragmented, app-centric controls

Healthcare organizations must classify PHI data in use, and not only when stored—it must be done inline across cloud, web, and private app traffic. A single set of policies should also apply across EHR exports, file sharing tools, cloud storage, and email. In addition, users should be coached or blocked when they try to move PHI unsafely, and AI or LLM tools must be treated as governed channels with appropriate guardrails.

Solution: Netskope DLP, CASB & AI governance (GDPR, HIPAA, EU AI Act)

- Netskope unifies DLP, CASB, and AI governance into single-pass inspection across SaaS, web, and IaaS, using 3,000+ healthcare identifiers to discover, classify, and protect PHI end to end.
- CASB and DLP controls prevent sensitive data from entering unapproved AI or cloud tools and redirect users to approved services, giving teams demonstrable control of AI risks.
- These capabilities directly support GDPR Data Protection by Design, HIPAA privacy and security obligations, and EU AI Act High-Risk system requirements.

Unified discovery, classification, and protection



Rule 4. Build resilience and response into the architecture, not around it

Most remote access solutions weren't built for always-on digital care, and they leave networks brittle. A single VPN concentrator, congested internet break-out, or overloaded on-premise security stack can slow or block access to clinical systems.

Incident response is spread across multiple consoles and manual steps, so even serious issues take too long to detect and contain.

This is what happens when resilience and response are add-ons rather than core architectural principles. Controls and automation get layered onto legacy networks instead of forming an integrated fabric.

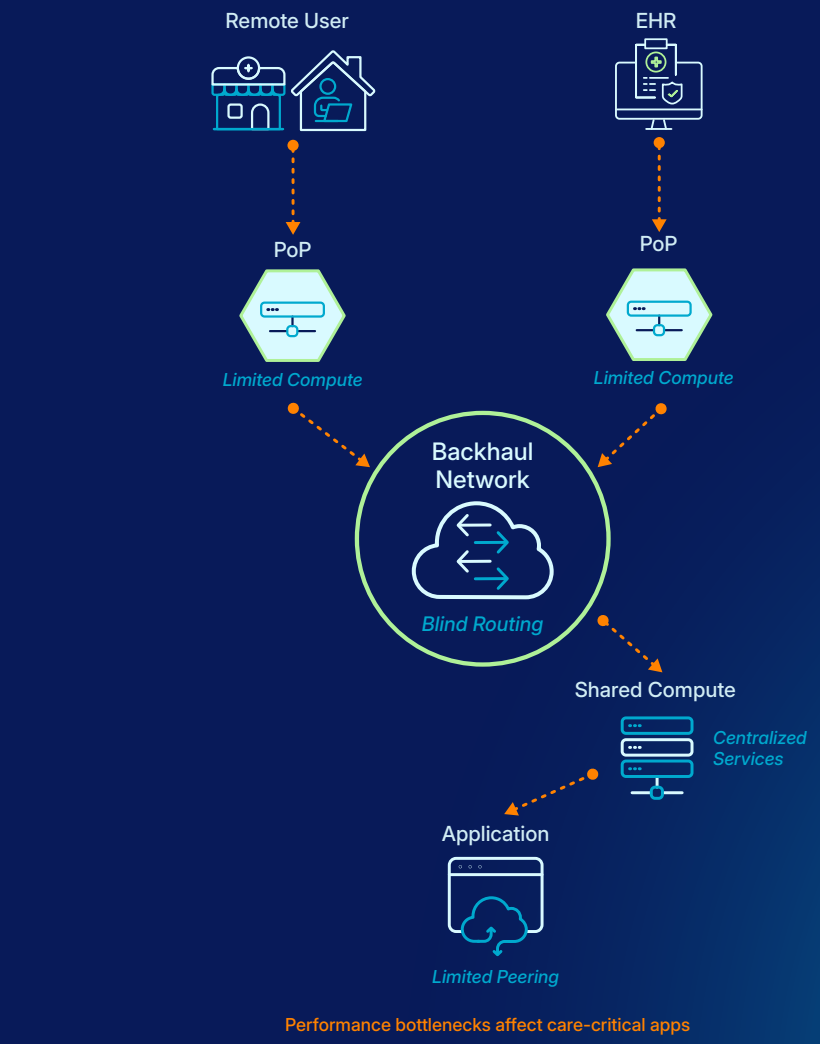
In that model, there is no performance guarantee for critical apps or prove response processes meet regulatory expectations.

The new imperative

A distributed access and security layer close to users and apps, with built-in redundancy and clear performance targets.

This requires a single source of truth for events, and analytics and playbooks that isolate risky users, revoke sensitive access and guide containment—making resilience predictable and repeatable.

Legacy hub-and-spoke architecture creates single points of failure



Healthcare organizations should move away from hub-and-spoke VPN models and toward a distributed secure-access fabric that applies dynamic controls close to users and applications. This reduces single points of failure and helps maintain stable performance for EHR, radiology imaging, and other clinical systems.

Security ecosystem telemetry should feed into unified analytics, with automated response workflows that trigger containment actions the moment unusual behavior is detected.

Solution: Netskope NewEdge* & Advanced Analytics (NIS2, HIPAA, GDPR)

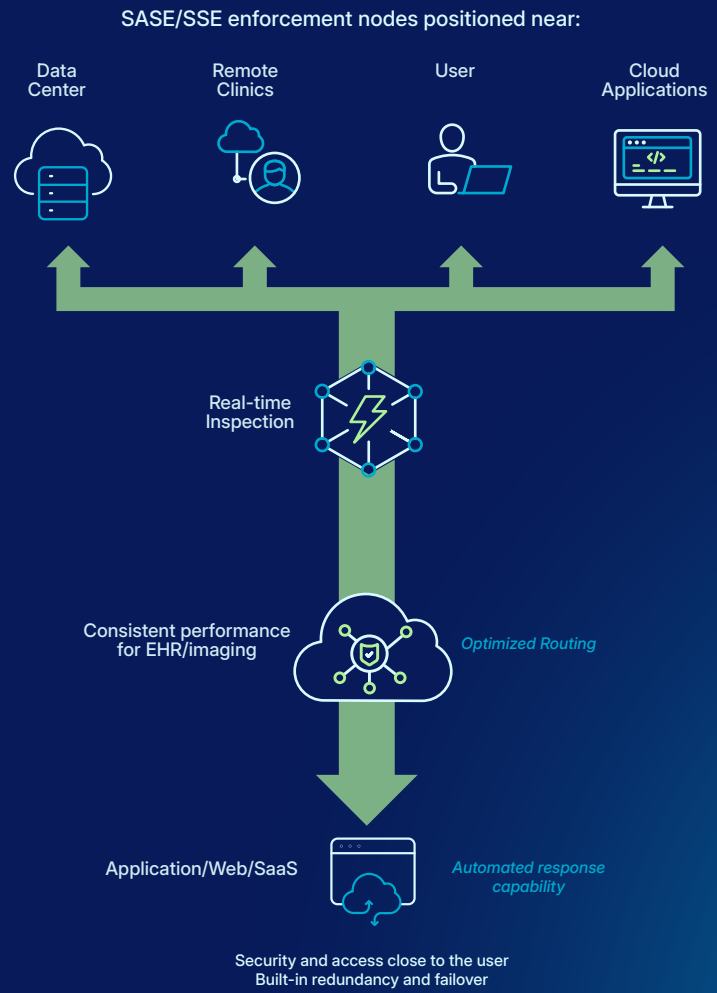
- Netskope's NewEdge Network provides 99.999% availability, low-latency enforcement, and removes VPN bottlenecks, supporting continuity expectations under NIS2 and HIPAA.
- Advanced Analytics gives a unified view of risk, accelerating detection and containment, while Cloud Exchange** automates ticketing, exporting log data, and sharing both threat and risk indicators to further enable SIEM/XDR workflows.
- Together, these strengthen architectural resilience and streamline incident handling under GDPR and NIS2.

Footnote:

**Netskope NewEdge, the world's most performant private security cloud, powers Netskope One. It delivers fast, secure access to data and apps with no performance trade-offs, purpose-built by experts as a hyperscale, SASE-ready network.*

***Netskope Cloud Exchange acts as an API broker to provide customers with powerful integration tools to leverage investments across their security posture.*

Distributed secure access fabric delivers resilience by design



Rule 5. Design for continuous audit readiness and change

For most healthcare teams, audits are still events and not part of routine processes. They trigger spreadsheet marathons, screenshot hunts, and last-minute scrambles to show which controls map to HIPAA, GDPR, NIS2, or local frameworks.

With every new partner, merger, EHR rollout, or regional expansion, the exercise repeats from scratch.

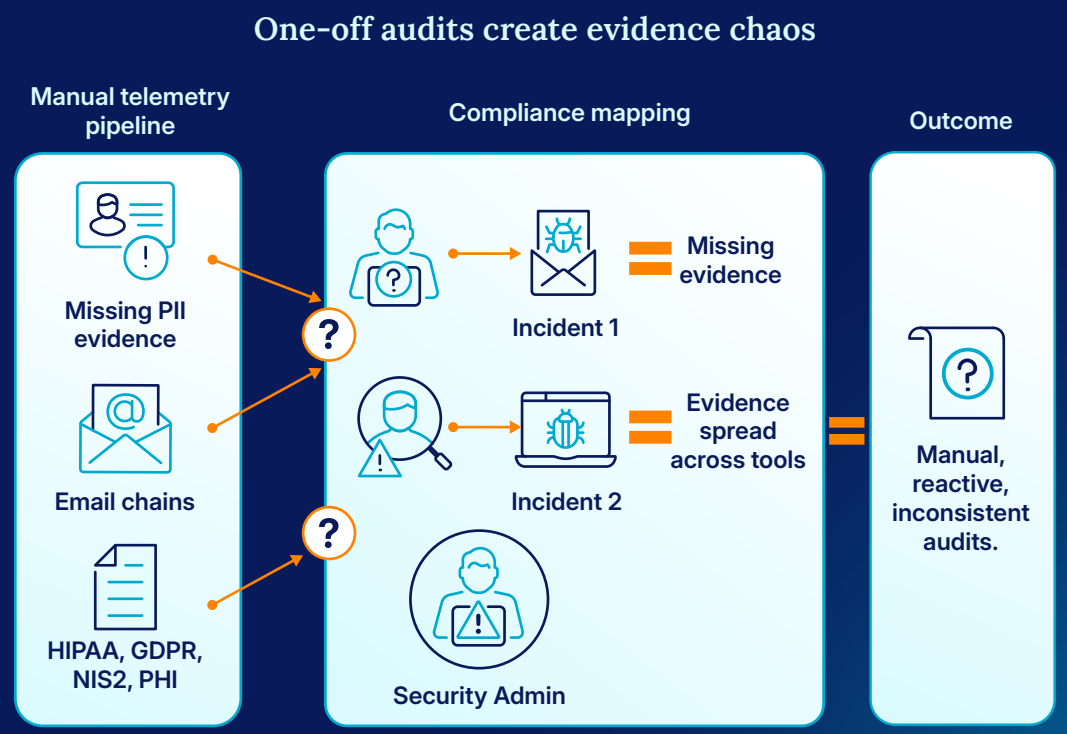
This happens when control-to-requirement mapping lives in isolated documents and institutional memory; policies are defined in one place, implemented in another, and evidenced somewhere else.

Without a single maintained view linking controls to frameworks, proving coverage is difficult, reuse is unlikely, and keeping ahead of regulatory change becomes nearly impossible.

The new imperative

Continuous compliance assumes organizations are always audit-ready, with line-by-line mappings between SASE and security controls and key frameworks, plus telemetry showing controls in action.

Evidence should emerge from daily operations, so new entities inherit proven policies. This turns audits from disruptive events into routine check-ins on a living control environment.



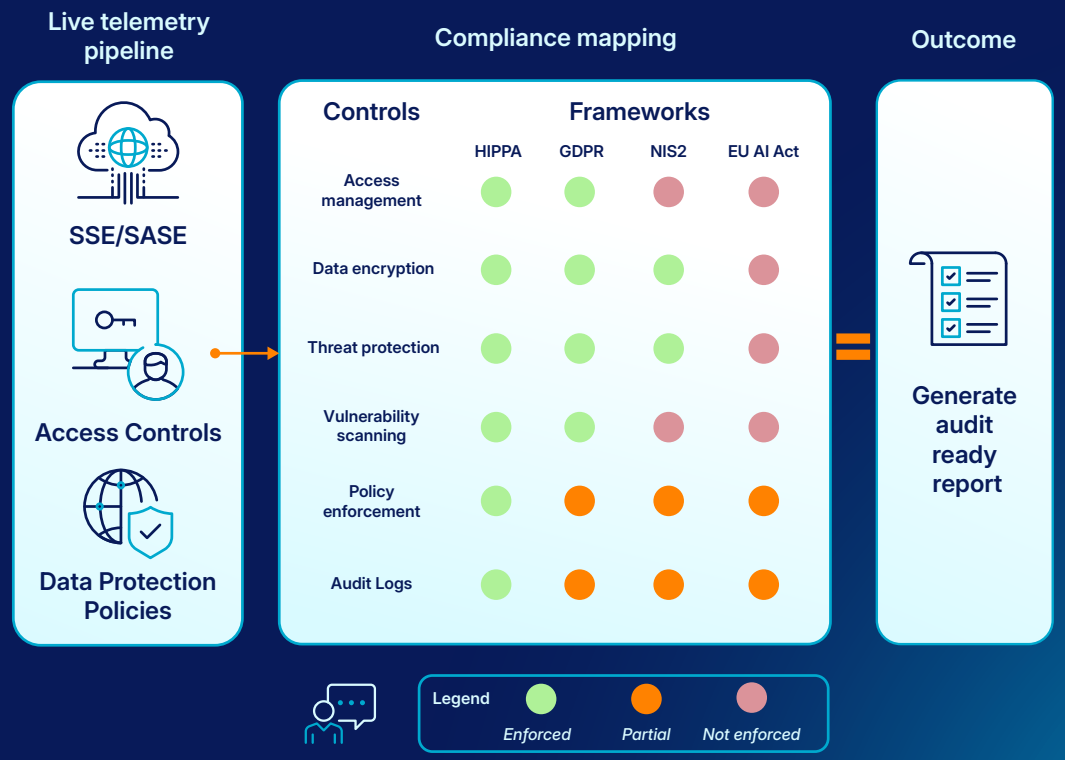
Healthcare organizations should maintain a central register that maps controls to key frameworks and is backed by real-time telemetry, enabling teams to answer “where is this enforced?” and “is it working?” without chasing evidence.

Using a single platform ensures new sites and partners inherit proven policies rather than rebuilding them from scratch. Audit reports can then be generated from day-to-day activity logs, policy histories, and configuration-drift insights.

Solution: Netskope One & continuous control mapping (HIPAA, GDPR, NIS2, NIST CSF, EU AI Act)

- Netskope One provides live, line-by-line mapping of SASE/SSE controls to HIPAA, GDPR, NIS2, NIST CSF, and the EU AI Act.
- Continuous telemetry generates evidence automatically, replacing manual reconstruction.
- Consistent controls extend across new sites, partners, and acquisitions, reducing integration labor and maintaining a unified security posture in line with the brief’s audit and operational efficiency outcomes.

Live, structured control-to-framework mapping



Conclusion - Keeping patient care at the center of risk, compliance, and continuity

Across this eBook, one theme has surfaced again and again: Continuous compliance is not just about satisfying auditors. It's about ensuring the digital systems that care depends on remain available, trustworthy, and safe for patients every day.

Regulations are being strengthened to reinforce this. In the U.S., HIPAA security, privacy, and breach-notification rules are now interpreted through a much stricter cybersecurity lens. Across Europe and beyond, frameworks such as NIS2, GDPR, and the EU AI Act are raising expectations for visibility, resilience, and incident reporting.

The five rules in this eBook point toward a different operating model, one in which real-time visibility serves as the foundation to build controls against the reality of PHI flows, not fitting to the way in which PHI appeared to flow during the last assessment. This enables a move from retrospective evidence-gathering to continuous assurance.

None of this removes the need for validation or judgment, but it does change where time goes. Instead of stitching together screenshots and spreadsheets, teams can focus on how controls perform in practice, how quickly they can adapt to new risks, and how well their digital environment supports safe care.

Continuous compliance isn't a box to tick. It's an ongoing commitment to align risk, compliance, and continuity so clinicians can deliver the best possible care. When teams have confidence that the data and systems they rely on are protected every hour of every day, they can focus on what really matters: delivering patient care.

Netskope's zero trust-powered SASE architecture supports this model by unifying access control, data protection, AI governance, and resilience in a single platform aligned with HIPAA, NIS2, GDPR, NIST CSF, and the EU AI Act, making continuous compliance something healthcare organizations can demonstrate in real time.

Download Netskope's compliance guides to map the capabilities of Netskope One to GDPR, NIS2, and more.

To see how the Netskope One platform supports your compliance requirements, book a demo here.

About Netskope

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.

Interested in learning more?

Request a demo