netskope
+ for Healthcare

White Paper +

Risk. Compliance. Continuity.

A unified blueprint for modern healthcare security

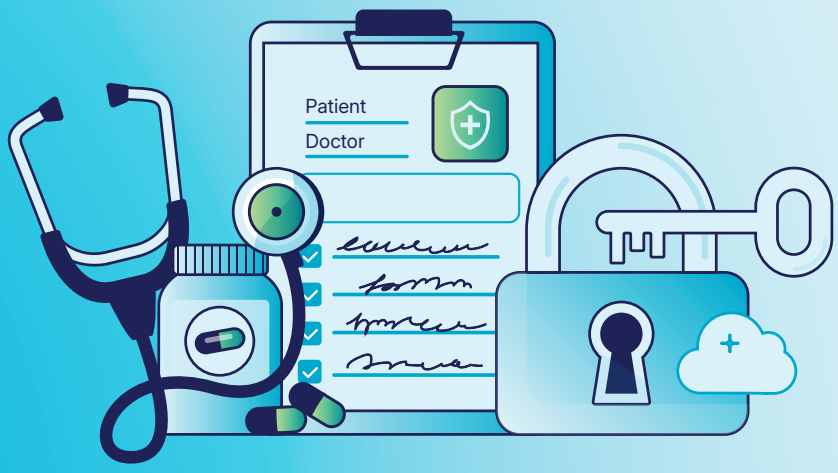


Table of Contents

THE MODERNIZATION MANDATE COLLIDES WITH RISK

The healthcare industry has reached a critical inflection point. Opportunity and risk are converging, forcing leaders to make choices that will shape patient care for years to come.

For healthcare leaders, the pressure to modernize is intense, driven by patients wanting connected, intuitive experiences; clinicians seeking relief from repetitive tasks; and organizations striving to optimize operations and grow. These needs are pushing the widespread adoption of electronic health records (EHRs), cloud platforms, connected medical devices, and AI, reshaping how care is delivered and how data is shared.

However, while the need to digitally transform is pressing, cyberattacks remain the dominant threat looming over these organizations.

Healthcare has become the most targeted industry for cyber criminals[1], and it is not hard to see why. Hospitals and patient care are increasingly dependent upon uninterrupted access to digitized clinical and administrative systems. And digital health records contain a full spectrum of Personally Identifiable Information (PII)—medical histories, insurance details, and financial information—that can be exploited in bulk as well as on an individual level.

A single breach can potentially cost an organization millions of dollars in penalties, however (and perhaps uniquely among sectors), the real impact is measured in lives disrupted when critical services are stalled. The 2024 Change Healthcare attack[2] triggered nationwide disruption to claims, payments, and e-prescribing workflows—further endangering patients and impacting other hospitals. It was a stark reminder that cyber incidents are not just IT problems; they're patient safety issues.

Legacy systems and technical debt have become shackles that constrain modernization efforts. Decades-old EHR systems, mainframes, and custom apps are difficult to patch or integrate, while pandemic-era quick fixes—most notably VPNs bolted onto aging networks—have left behind brittleness and security gaps. The result is a sprawl of overlapping vendors and appliances that add overhead, fragment policies, and inflate costs—undermining the "always-on" reliability healthcare systems depend on, and ultimately, putting patient care at risk.

Globally within the healthcare sector, the challenge of protecting digital systems and the data they contain is amplified by countless interfaces across the Internet of Medical Things (IoMT).

Thousands of connected devices—such as monitors, pumps, and scanners—are difficult to update or secure consistently. Layer on the rise of AI applications—such as AI-enabled apps that record and transcribe clinician and patient conversations—and the attack surface grows even wider, introducing new vectors for data exposure and elevated operational risk.

So, with regulators tightening requirements, clinicians demanding systems access from anywhere, and patients expecting seamless experiences, the challenge has been laid out for leaders: How do you secure all this complexity without interrupting care or introducing friction across the user experience?

This whitepaper is built around three strategic imperatives: **risk, compliance, and continuity**. Taken together, these imperatives point to the future of modern healthcare security—one built on zero trust principles and a unified SASE architecture. Far from being obstacles, these frameworks will form the foundation for safe, compliant, and uninterrupted patient care in an increasingly digital, AI-enabled health ecosystem.

Healthcare organizations are under pressure to:

- **Defend against attacks:** ransomware, insider threats, and third-party exposure across cloud, SaaS, and IoMT environments
- **Prove compliance:** meet HIPAA, NIS2, the EU Cyber Resilience Act, and emerging U.S. rules, with real-time visibility and automated evidence
- **Keep care flowing:** ensure clinicians can access critical systems like Epic and Cerner—leading electronic health record (EHR) platforms—without delay, and integrate new models or mergers and acquisitions securely

1. https://health-isac.org/wp-content/uploads/Health-ISAC_2025-Annual-Threat-Report.pdf?
2.https://www.reuters.com/business/healthcare-pharmaceuticals/change-healthcare-network-hit-by-cybersecurity-attack-2024-02-22/

Strategic Imperative: Protecting patient data and defending care delivery from converging threats

When it comes to risk in healthcare, the impact goes far beyond compliance fines or reputational harm. It can be measured in lives put in jeopardy when critical systems are disrupted, and the trust that's often irreparably lost when sensitive health records are stolen or leaked.

Ransomware—malicious software that encrypts and locks critical patient data or operational systems, ostensibly until a payment is made—is a particular problem for healthcare, and the most frequently targeted sector in 2023 and 2024[3]. The leverage ransomware gives attackers is immense: Once clinicians are blocked from essential tools or patients are forced to delay treatment, the pressure on leadership to pay becomes overwhelming.

And when attacks on healthcare organizations succeed, they carry the highest financial toll of any industry. Beyond potential ransom demands, healthcare organizations face the spiraling costs of recovery, legal fees, regulatory fines, and the reputational damage that erodes patient trust. Worse still, paying a ransom can inadvertently fuel the very criminal networks behind these attacks, amplifying the threat across the sector.

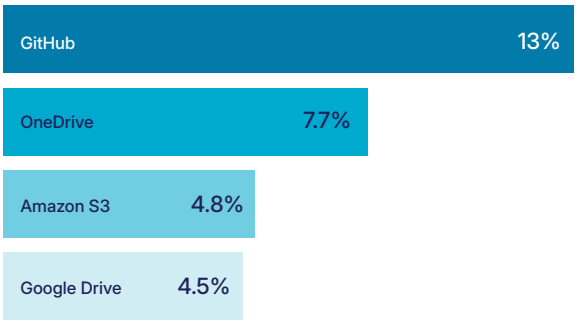
Ransomware isn't the only type of attack being mounted on the sector. Adversaries are combining data theft, extortion, and service disruption into multi-pronged attacks, and using trusted cloud apps as delivery channels. In 2025, GitHub emerged as the leading source of malware downloads in healthcare, with 13% of organizations experiencing monthly incidents—followed closely by popular storage platforms such as Microsoft OneDrive, Amazon S3, and Google Drive[4].

Insider and third-party exposure add another layer of vulnerability, as overstretched staff, contractors, and business associates all become potential entry points for attackers. Data policy violations show how easily this risk materializes: 81% of violations in healthcare involve regulated data uploaded to unapproved web or cloud destinations, underscoring the critical need for stronger data loss prevention (DLP) controls[4].

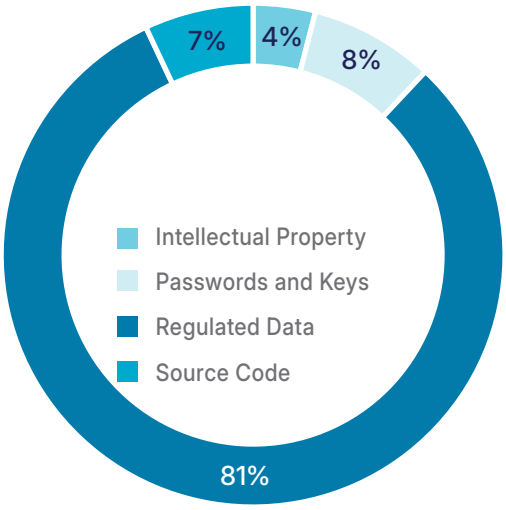
More recently, the growing use of AI is creating new risks through the leakage of sensitive data in prompts, outputs, and shadow tools. Adoption is now nearly universal: 88% of healthcare organizations use cloud-based AI apps, 96% rely on apps that train AI models with user data, and 98% have adopted apps with embedded AI features[4].

As AI's usage spreads, a growing share of sensitive data—including regulated data, source code, and intellectual property—is being exposed.

Top apps for malware downloads in healthcare sector



Type of data policy violations in the healthcare sector



3. https://health-isac.org/wp-content/uploads/Health-ISAC_2025-Annual-Threat-Report.pdf
4. https://www.netskope.com/resources/threat-labs-reports/threat-labs-report-healthcare-2025

Seen together, these risks form a complex, converging picture that traditional perimeter defenses or point solutions are ill-equipped to handle. What healthcare organizations need instead is a unified, data-centric model of protection; one that adapts to real-time signals, applies consistent policy everywhere, and reduces the likelihood that a single misstep can cascade into a crisis.

The modern blueprint

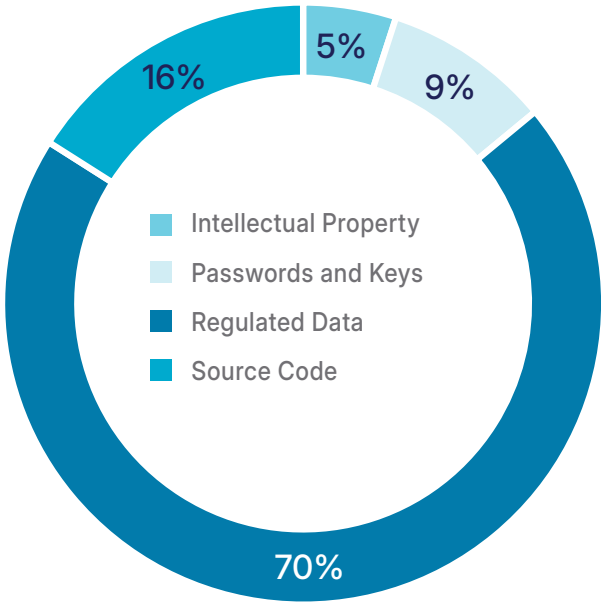
To avoid recreating today's complexity quagmire, organizations must avoid simply bolting new controls onto legacy systems. Fragmented stacks of point solutions are what introduced blind spots, inconsistent policies, and unnecessary overhead in the first place. A truly unified approach must instead close those gaps through seamless integrations, scale with demand, and adapt to the real-time context of users, devices, and data.

A unified secure access service edge (SASE) platform resolves these challenges by consolidating key network and data protection capabilities—bringing together secure web gateway (SWG), cloud access security broker (CASB), data loss prevention (DLP), zero trust network access (ZTNA), Firewall as a Service (FWaaS), and software-defined wide area network (SD-WAN) into a single, cloud-delivered architecture.

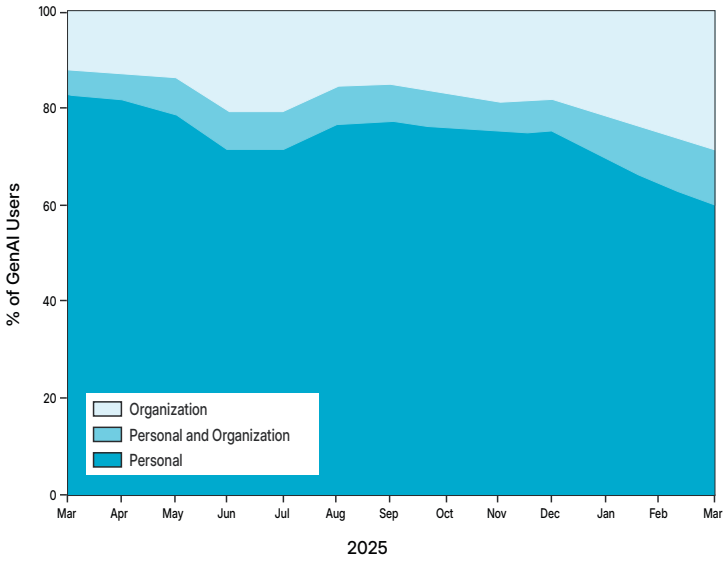
At the heart of this model, the zero trust architecture is capable of continuously evaluating context and adapting access policies accordingly. So, instead of relying on static or binary permissions, decisions can be made in real time, based on user identity and behavior, device posture, location, data sensitivity, and activity. This ensures that clinicians, contractors, and third parties are granted only the access they need, when they need it, and no more.

Inline data protection through advanced DLP and data security posture management (DSPM) is equally critical. These capabilities enable deep inspection across cloud, SaaS, and web traffic, using thousands of identifiers to recognize and safeguard personal health information (PHI). These same controls also detect uploads of regulated data, source code, or intellectual property to unapproved locations—including personal app instances and AI tools—preventing inadvertent leakage before it occurs.

Data policy violations for personal apps in the healthcare sector

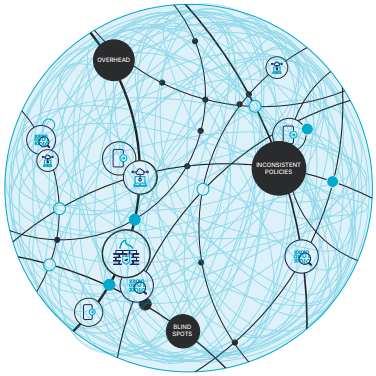


GenAI usage personal vs. organization account breakdown in the healthcare sector



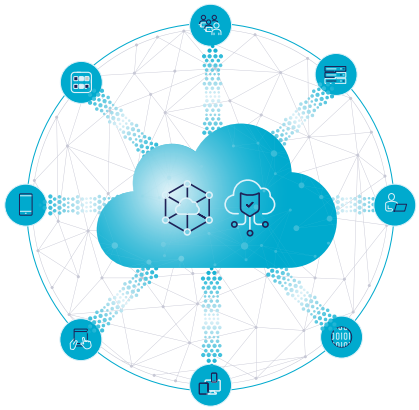
Before

Reactive, perimeter-based defenses relying on implicit trust



After

Unified, adaptive zero trust protecting data everywhere.



With a unified security service edge (SSE) or SASE platform, healthcare organizations can consolidate multiple point products into a single control environment, reducing the risk of misconfiguration, closing policy gaps, and lowering costs, while providing IT and security teams with a consolidated view of activity across the entire environment. So, instead of constantly wrestling with overlapping tools, security teams can focus on proactive risk management.

Advanced threat protection (ATP) further strengthens this defense by inspecting all HTTP and HTTPS traffic—including downloads from cloud and web apps—to identify phishing attempts, malware, and zero-day exploits that would otherwise slip through. With attackers now regularly exploiting trusted apps such as GitHub or OneDrive for malware distribution, this inspection is vital.

Forrester's composite organization achieved these savings through:

- Enhanced protection against malware
- Tightened DLP controls
- Improved visibility into and context for risky user behaviors
- Stronger security controls to block risk behaviors before they do harm
- Lower security incident volumes and accelerated breach resolution times

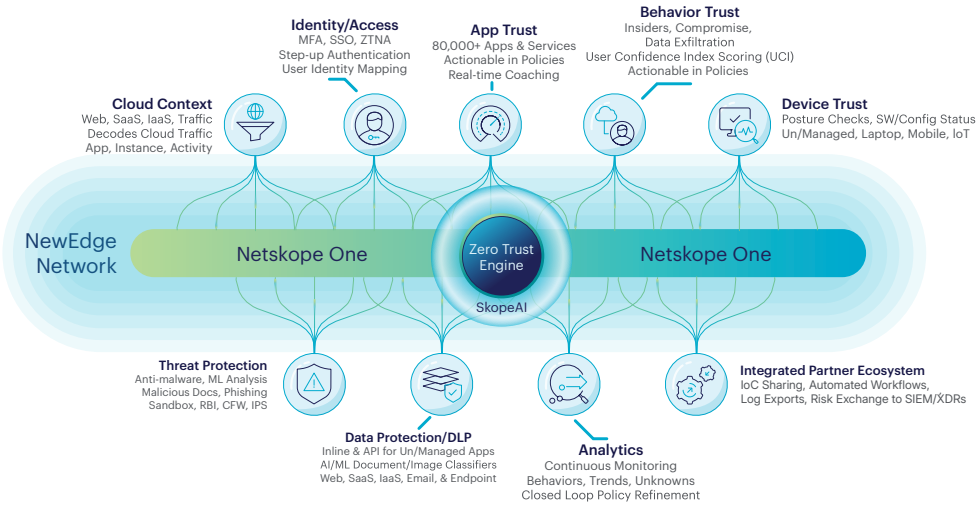
To address the risk surface issue presented by the IoMT organizations can minimize lateral movement and contain potential breaches before they escalate by segmenting and monitoring connected devices under zero trust principles.

And finally, in scenarios where clinicians do have to visit high-risk or newly registered domains, remote browser isolation (RBI) provides an additional safeguard by isolating browsing sessions from the core infrastructure. Data security is reinforced through DLP policies that govern file activity—safely enabling uploads and downloads from isolated websites and applications. Remote Browser Isolation's read-only mode also prevents users from typing or leaking information, and clipboard, copy/paste, and print controls ensure that sensitive data stays protected.

All in all, this combination of controls builds a security model that protects critical systems and keeps care seamless.

Key elements:

1. **Unified SSE/SASE platform—**to collapse point products, close policy gaps, and simplify operations
   - **Adaptive access control—**through zero trust architecture, informed by real-time signals
   - **Inline DLP and DSPM—**to safeguard PHI, regulated data, and sensitive assets across SaaS, web, and AI apps
   - **Remote Browser Isolation (RBI)—**an added layer of protection for contractors, high-risk use cases or untrusted sites
2. **IoMT segmentation and monitoring—**to contain lateral movement across connected devices



Adaptive risk-based framework

A unified risk model enables CISOs and CIOs to show measurable reductions in exposure—up to 80% through platform consolidation[5] — while assuring their board and regulators that patient data, clinical systems, and connected devices are consistently protected. For healthcare, that translates into fewer breaches, faster response times, and above all, confidence that a security failure will never compromise patient safety.

COMPLIANCE

Strategic imperative: maintaining trust through consistent, audit-ready controls

Compliance is about more than just meeting legal requirements; in healthcare, it is the foundation of trust between patients, providers, and regulators. A breach that exposes protected health information does not only incur costly fines, it also damages patient confidence, which often leads to lawsuits, class actions, and long-lasting reputational harm.

Regulatory bodies are moving fast to adapt to the evolving threat landscape.

For example, while HIPAA remains the cornerstone of healthcare compliance in the U.S., the U.S. government has recently introduced updates and new proposals, such as the Healthcare Cybersecurity Act[6]. It aims to strengthen coordination between the Cybersecurity and Infrastructure Security Agency (CISA) and Health and Human Services (HHS), while expanding federal support with new tools, training, and threat intelligence—signalling stricter expectations for providers.

In Europe, NIS2[7] expanded its scope to healthcare with stricter incident-reporting timelines and heavier penalties, while the EU Cyber Resilience Act[8] mandates that medical devices and healthcare software must be secure-by-design.

In the APAC region, regulations are equally demanding. Australia's Privacy Act and Australian Privacy Principles (APPs)[9] require any organization operating in Australia, or handling Australian data, to meet strict standards for consent, breach notification, and data governance. Meanwhile, Singapore's Personal Data Protection Act (PDPA)[10] enforces similar safeguards for personal and health information, emphasizing accountability and rapid incident reporting.

For healthcare providers operating across international borders, the compliance challenge multiplies exponentially as they navigate overlapping obligations across numerous jurisdictions without compromising care delivery or security.

The industry has moved beyond the era when compliance could be proven once a year during an audit. Regulators and patients alike now expect continuous assurance that controls are in place and working effectively. Manual evidence collection is too slow and resource-intensive for overstretched compliance teams, and too often leaves gaps that adversaries can exploit.

What's needed instead is automated, audit-ready reporting that demonstrates adherence in real time. By embedding compliance into daily operations, healthcare organizations can move from a reactive, box-ticking approach to proactively protecting both patients and their data.

5. https://www.netskope.com/blog/the-total-economic-impact-of-netskope-sse 6. https://www.infosecurity-magazine.com/news/congress-bill-healthcare/ 7. https://www.nis-2-directive.com/ 8. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act 9. https://www.oaic.gov.au/privacy/australian-privacy-principles 10. https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act

REGULATION	JURISDICTION	KEY IMPLICATIONS/ REQUIREMENTS
HIPAA	**USA**	2025 updates impose higher fines, stricter controls (e.g., MFA, encryption, testing), 15-day patient record access, and updated vendor management requirements
HISAA (proposed)	**USA**	The proposed HISAA bill aims to address limitations within HIPAA by introducing mandatory minimum cybersecurity standards, financial aid, and executive accountability
Healthcare Cybersecurity Act (proposed)	**USA**	Stronger CISA–HHS coordination, federal tools/training, sector risk assessments
NIS2 Directive	**EU**	Healthcare in scope, 24-hour incident reporting, strict risk management, fines up to €10M/2% turnove
Cyber Resilience Act	**EU**	Secure-by-design rules for digital products and medical devices, ongoing update obligations
EU Action Plan (2026)	**EU**	EU-wide early warning service, cyber incident reserve, voluntary medical device vulnerability reporting
Australia's Privacy Act and Australian Privacy Principles (APPs)	**APAC**	Governs how organizations handle personal information, emphasizing transparency and security
Singapore's Personal Data Protection Act (PDPA)	**APAC**	Regulates the collection and use of personal data, ensuring accountability, consent, and breach notification

The modern blueprint

Meeting today's compliance expectations requires more than static controls and manual audits. Healthcare organizations need their compliance model integrated into daily operations—consistently enforcing policy across every system, automating evidence collection, and providing continuous assurance to regulators, patients, and boards alike.

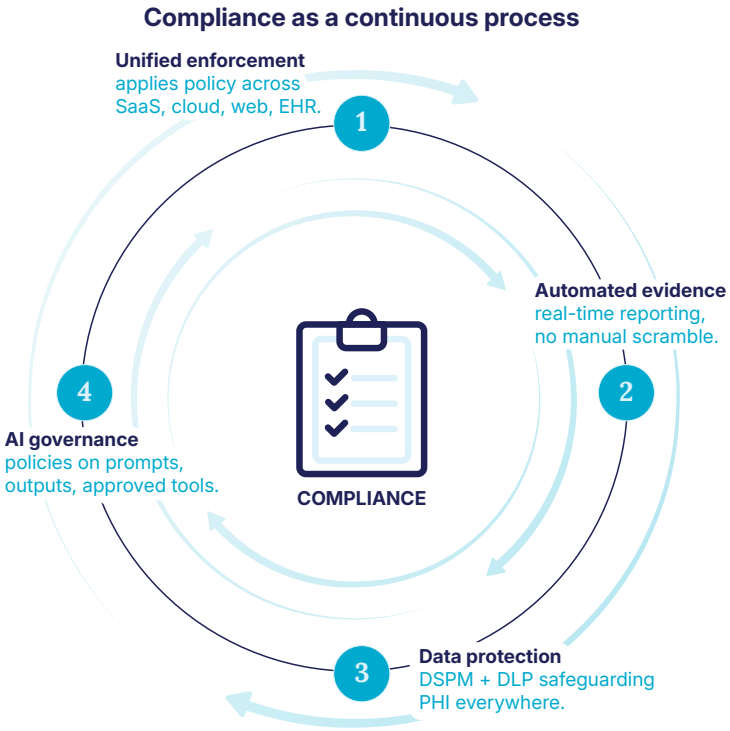
At the heart of this approach is consistent, policy-driven enforcement. So, instead of relying on siloed tools, healthcare organizations should implement a unified platform that applies the same rules everywhere: across SaaS applications, web traffic, device, location, cloud platforms, and electronic health record (EHR) systems mapped to the user/persona accessing those resources. This reduces the likelihood of gaps and misconfigurations, making compliance easier to demonstrate.

Automated evidence and audit-ready reporting mean compliance teams no longer need to scramble for logs and screenshots during an audit. Instead, they can generate real-time reports that prove who accessed what, when, and under which conditions. This shift not only reduces audit fatigue but also shows regulators that security is continuous.

With inline data protection and visibility, DSPM and advanced DLP controls safeguard PHI wherever it travels—across cloud services, collaboration platforms, and even personal or unapproved applications. By catching uploads of regulated data, source code, or intellectual property to unauthorized destinations, organizations can prevent the violations that most often trigger regulatory penalties. Applying the data protection and visibility controls across third-party users and their devices needs to be factored into a unified and compliant IT security technology stack.

Finally, compliance can now extend into the governance of AI. With adoption nearly universal in healthcare, organizations need to be able to distinguish between approved and unapproved tools, block shadow usage, and apply policies to prompts and outputs to prevent inadvertent exposure of sensitive data. By embedding DLP and policy controls into AI workflows, leaders can capture the efficiency benefits of AI without introducing new compliance liabilities.

Collectively, this modern approach transforms compliance into a proactive system of assurance—one that protects patients, satisfies regulators, and frees overstretched compliance teams to focus on strategy rather than manual reporting.



Key elements:

- **Consistent policy enforcement**—applied seamlessly across SaaS, device, users, location, cloud, web, and EHR systems
- **Automated, audit-ready reporting**—delivering real-time proof of compliance without manual evidence collection
- **Inline DLP and DSPM**—protecting PHI, regulated data, and sensitive assets across approved and unapproved destinations
- **AI governance**—blocking shadow tools, applying policies to prompts and outputs, and monitoring AI usage
- **Unified platform controls**—reducing misconfigurations, closing policy gaps, and simplifying compliance operations

Compliance benefits

A modern compliance model enables compliance and privacy officers to move beyond reactive reporting and demonstrate continuous assurance. By unifying controls and automating evidence, they can reduce audit fatigue, minimize the likelihood of penalties, and strengthen patient trust. For healthcare providers, this means fewer regulatory surprises, smoother audits, and greater confidence that data is being handled responsibly across all systems.

Strategic imperative: uninterrupted care

In healthcare, continuity is not a nice-to-have—it's essential to patient safety. Even a few minutes of downtime can delay diagnoses, disrupt treatment plans, or prevent clinicians from accessing critical records.

And the effects ripple far beyond the clinic: providers may be unable to bill, patients can be left waiting for medications or results, and care teams forced to coordinate treatment without the systems on which they rely. Often, what begins as a technical outage can quickly escalate into both a clinical and financial crisis.

Against this backdrop, continuity has become a strategic imperative. Healthcare organizations must ensure secure, seamless access for clinicians and contractors, maintain high performance in core systems such as Epic and Cerner, and recover quickly in the event of incidents.

Yet legacy infrastructures—VPNs, brittle interconnects, and unmonitored device sprawl—were never built with resilience in mind. For years, VPNs were the standard way to connect clinicians, contractors, and third parties to critical systems. In today's complex healthcare environment, with the shift to remote doctor-to-patient meetings and the advent of accessing care from a mobile phone, they create single points of failure, struggle under the demands of distributed access, and often grant users broader privileges than necessary.

The result is friction at the worst possible moments, with clinicians facing delays logging in, dropped connections, or repeated re-authentication requests during a shift. Each interruption erodes productivity and adds stress in environments where every second counts and touch-and-go is the new standard for accessing internal resources. For care teams, these delays translate into longer patient waiting times, disrupted workflows, and critical records unavailable when decisions must be made.

Instead of enabling continuity, VPNs too often undermine it—creating bottlenecks that slow the delivery of care and widen the gap between clinical needs and IT capabilities. It's time for those bottlenecks to be replaced with systems designed to keep care flowing, no matter what happens.

Case study: AI system manipulation

In 2024, researchers at Asan Medical Center in South Korea trained a large language model on the medical records of more than 26,000 patients. By crafting malicious encoded prompts, they bypassed the model's security measures and forced it to expose sensitive data. The "guardrail deactivation rate" reached 80.8%, highlighting how easily AI systems can be manipulated in a clinical context[11].

For healthcare providers, the risk is not just data leakage but disruption of care workflows. If clinicians lose confidence in AI tools or have to pause critical systems after a breach, continuity suffers.

Remember: AI governance is not only a security imperative, but a continuity one.

The modern blueprint

More than keeping systems online, ensuring continuity in healthcare requires a security model that preserves the speed and reliability clinicians need while fortifying resilience against disruption.

Instead of relying on brittle infrastructure and siloed tools, healthcare organizations need integrated controls that make secure access invisible, protect performance, and provide a safety net when incidents occur.

The foundation is an adaptive zero trust framework, replacing VPNs with granular, context-aware connections that provide users with the right access at the right time. This gives clinicians and contractors precisely the access they need—without the excess privileges or single points of failure that undermine continuity. Access decisions adapt in real time to user, device, and data context, ensuring connectivity is both seamless and secure.

11. https://www.biotech-now.co.uk/article/158115/large-language-models-risk-security-breaches-when-applied-to-healthcare

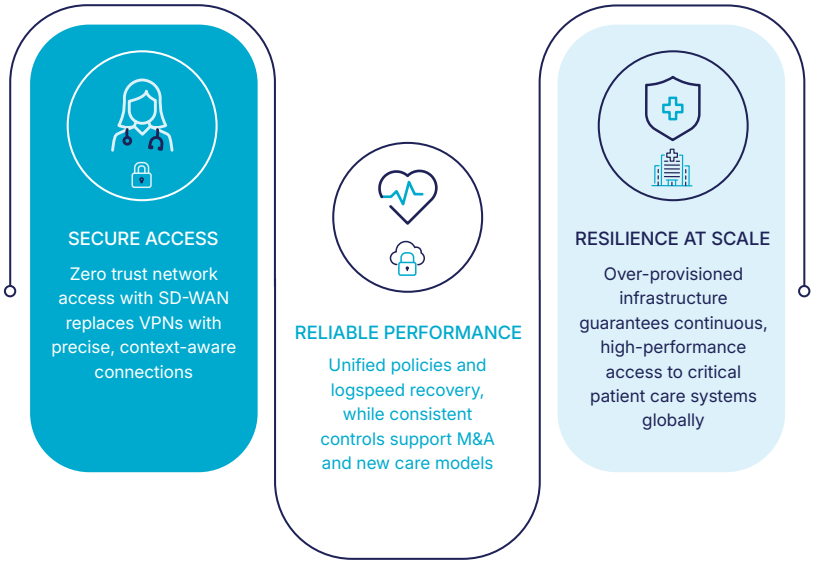
The approach extends across both managed and unmanaged devices, enabling secure, native browsing for contractors or temporary staff who may not be able to run a full client. This enterprise browser model delivers lower total cost of ownership (TCO) and enhanced control, ensuring consistent protection for every endpoint accessing healthcare data.

A resilient networking model, backed by distributed points of presence and intelligent traffic steering, ensures that performance never has to be sacrificed. By delivering low-latency access into core systems such as Epic and Cerner, and pairing it with digital experience management (DEM), IT teams gain end-to-end visibility to track user performance, spotting and resolving issues before they disrupt patient care.

When disruptions do occur, unified policies and centralized logging make it faster to contain threats, restore services, and demonstrate to regulators that the right processes were followed. This reduces both the operational and compliance impact of an incident.

Aside from incident readiness, continuity must extend beyond day-to-day operations. Mergers, acquisitions, and new care models are a constant in healthcare, each introducing new systems and users into the environment. A unified platform—anchored on zero trust access—accelerates integration by extending consistent policies across inherited systems, ensuring growth doesn't come at the expense of stability.

All together, these capabilities enable healthcare leaders to deliver on the most fundamental promise of continuity: that a security failure will never compromise patient care.



Key elements of a modern continuity approach:

- **Zero trust network access (ZTNA)**—replacing brittle VPNs with granular, context-aware connections
- **Resilient networking**—globally distributed points of presence to ensure low-latency access into core systems such as Epic and Cerner
- **Digital experience management (DEM)**—end-to-end visibility to spot and resolve performance issues before they disrupt care
- **Unified policies and logging**—faster containment, recovery, and audit readiness when incidents occur
- **Seamless integration to the healthcare ecosystem**—extending consistent policies across new systems during mergers, acquisitions, care-model changes, and emerging technologies

Continuity benefits

A modern continuity model enables CIOs, CMIOs, and IT leaders to keep care flowing under any condition. By unifying access, networking, monitoring, and incident response, it can reduce downtime, accelerate recovery, and maintain consistent performance across the systems clinicians rely on most. For healthcare, that means fewer interruptions, faster integration of new services, and confidence that security will never come at the expense of patient care.

RISK, COMPLIANCE, CONTINUITY: WHEN SECURITY SAFEGUARDS CARE

Healthcare security evolves in cycles of investment, and many organizations are now reaching a point where legacy choices are showing their limits. These cycles are often reactive, prompted by breaches within their own networks or in neighboring organizations. VPNs once felt transformative, and few predicted how much cloud, IoMT, and AI would reshape the sector in just a few years.

Today, leaders have the opportunity to build on those earlier investments and take the next step—consolidating onto integrated platforms that protect data, satisfy regulators, and preserve the flow of care without compromise.

This means every healthcare strategy must now begin with proactive risk control. Addressing ransomware, insider misuse, and third-party exposure creates the foundation for consistent threat and data protection and policy enforcement across cloud, SaaS, and IoMT environments. From this baseline, organizations can begin to better assure the board, regulators, and patients that sensitive health data remains safe.

Once that foundation is in place, leaders can turn their focus to embedding compliance seamlessly across every system and workflow. Instead of exhausting staff with manual reporting cycles and fragmented evidence, a unified platform automates audit readiness and applies one set of policies across jurisdictions. HIPAA, NIS2, and the EU Cyber Resilience Act can then become part of daily operations rather than annual crises—transforming regulatory pressure into a system of continuous assurance.

Once risk and compliance are addressed, organizations can have confidence in their ability to deliver true continuity. By replacing brittle VPNs with ZTNA and SD-WAN, ensuring low-latency connectivity into core systems such as Epic and Cerner, and embedding resilience through distributed networking and DEM, security shifts from obstacle to enabler—quietly powering uninterrupted patient care.

Together, **risk, compliance,** and **continuity** form a blueprint for modern healthcare security that not only protects data and systems but safeguards the trust at the heart of every care interaction. The objective is not simply to contain threats, but to give clinicians the confidence that they can deliver safe, connected, and uninterrupted care—no matter how the threat landscape evolves.

Mapping the blueprint

- **Risk (unified control)**—One control plane for PHI, cloud, SaaS, and AI, shifting from reactive tickets to predictive controls and continuous audit readiness
- **Compliance (audit-ready by design)**—Automated evidence, consistent DLP, and policy frameworks that align with HIPAA, NIS2, CRA, and emerging regulations
- **Continuity (no trade-offs)**—Zero trust network access, distributed points of presence, and digital experience monitoring that keep clinicians connected without adding friction

Key shifts that make this real

- Point products and manual evidence → Unified platform policies, real-time signals and context
- Perimeter-centric access → Data-centric zero trust everywhere people work
- VPN backhaul and brittle interconnects → Direct-to-cloud access via private SASE
- Siloed security and risk management → Converged threat and behavioral intelligence
- Shadow AI and ad hoc guardrails → Approved AI with usage and data governance

Architectural principles to hold

- **Single-pass inspection and unified policy**—across web, cloud, and private apps, lower latency, and fewer inconsistencies
- **Cloud-native scale and distributed POPs**—resilient performance through outages or surges
- **Extensive peering and optimized connections**—high-performance connectivity across regions
- **AI-ready policy framework**—govern prompts, models, and APIs without re-architecting
- **Deep observability and digital experience management (DEM)**—track experience and resolve issues before they disrupt care

Measurable impact in quarter one

- **Boards and regulators**: Assurance that maps to measurable outcomes. Overlapping or redundant controls are eliminated, audit response cycles shortened, and shadow AI governed.
- **Clinicians and patients**: Seamless access to records and apps without disruption. Continuity reinforced even during outages or cyber incidents.
- **IT and compliance teams**: Less manual evidence gathering, fewer hand-offs, and faster remediation. Time reclaimed for proactive initiatives.
- **Culture and talent**: A modern platform that reduces toil, attracts digital-first talent, and reinforces a mindset of safe innovation.

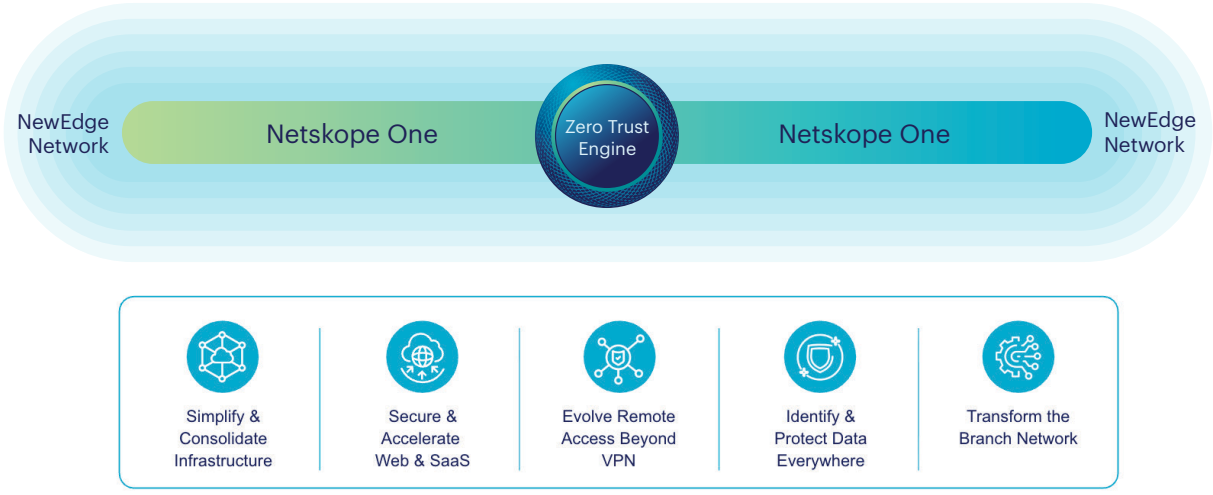
Building from the blueprint

Risk, compliance, and continuity may form the blueprint of a modern healthcare security strategy, but no one can live in a drawing. Turning that blueprint for a "house" into real "rooms" requires practical use cases and integrations that bring the strategy to life.

In practice, this means safeguarding PHI everywhere, governing AI use, defending against cloud-delivered threats, and ensuring performance through a private SASE cloud with distributed POPs. It also means applying automated guardrails, user coaching, and localization controls to address insider risk and data residency requirements—reinforcing a culture of security that doesn't slow care delivery.

With Netskope, the vision for healthcare security moves from concept to execution. Through deep integrations with Imprivata, Epic, Microsoft, ServiceNow, and CrowdStrike, Netskope turns strategy into action—automating evidence collection, securing and verifying access to critical patient systems, and delivering consistent enforcement across cloud and web traffic. The result is a resilient, unified foundation for safe, connected, and uninterrupted patient care.

With a modernized approach to risk, compliance, and continuity, healthcare leaders can secure today and prepare for tomorrow with one platform, one policy, and no trade-offs.



Visit Netskope.com/ for real-world healthcare use cases and customer success stories.

Ready to learn more?

Request a demo

Netskope, a global SASE leader, helps organizations apply zero trust principles and AI/ML innovations to protect data and defend against cyber threats. Fast and easy to use, the Netskope One platform and its patented Zero Trust Engine provide optimized access and real-time security for people, devices, and data anywhere they go. Thousands of customers trust Netskope and its powerful NewEdge network to reduce risk and gain unrivaled visibility into any cloud, web, and private application activity—providing security and accelerating performance without compromise. Learn more at netskope.com.