netskope

White Paper

Building a Secure and Resilient Healthcare Enterprise

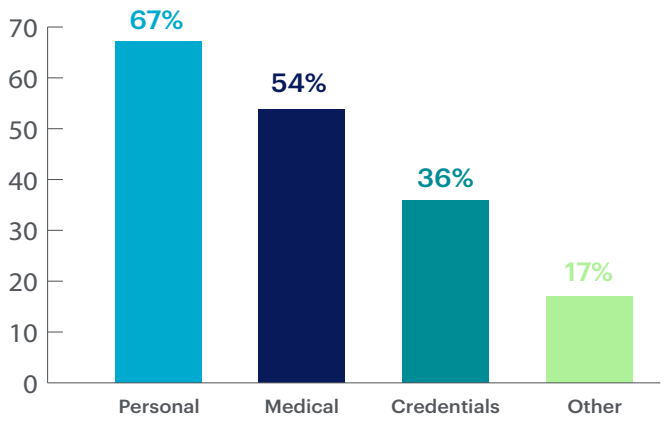
Netskope helps healthcare organizations protect patient privacy, support regulatory compliance, safely adopt new digital technologies, and ensure operational resiliency and effectiveness.

INTRODUCTION

Digital transformation is not a one-time event but an ongoing process that requires continuous investment, innovation, and adaptation to remain effective. To achieve success, healthcare organizations must adopt a digital-first mindset, prioritize patient needs, and invest in the right mix of technologies, people, and processes. Moreover, healthcare organizations must address the challenges posed by digital technology, including data privacy and security, interoperability, data governance, and data quality.

As healthcare becomes more digital, the need for robust cybersecurity measures has become even more critical. Between November 1, 2021, and October 31, 2022 there were 436 confirmed data breaches in the healthcare sector globally, with 67% compromising personal data, 54% medical data, and 36% credentials[1]. Healthcare organizations must ensure that their digital infrastructure is secure, resilient, and scalable to support the growing demands of patients and clinicians.

Digital transformation is a significant opportunity for healthcare organizations to improve the quality, safety, and efficiency of patient care while reducing costs and improving outcomes. By embracing digital technologies, healthcare organizations can transform the industry for the better, but this requires investment in the right mix of technologies, people, and processes, as well as robust cybersecurity measures to ensure data privacy and security.



Types of Data Compromised in Healthcare[1]

[1] Source: Verizon 2023 Data Breach Investigations Report

NAVIGATING THE DIGITAL TRANSFORMATION CHALLENGES IN HEALTHCARE

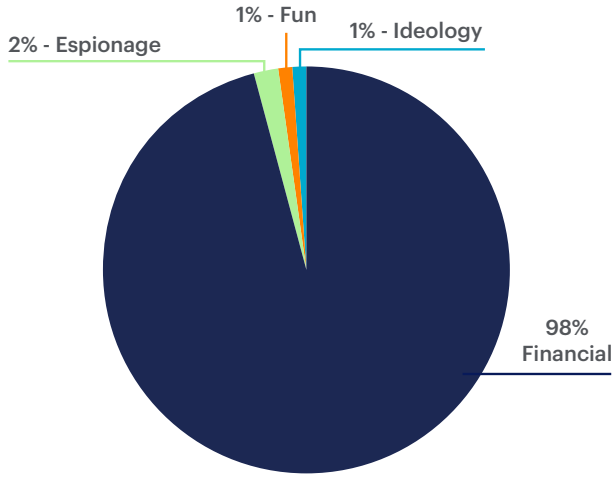
The rapid pace of technological development has created an expanding digital opportunity in healthcare. Electronic Medical Records (Electronic Health Records) Systems, for example, can improve clinicians' ability to understand patient history, diagnose conditions, and enhance the overall efficiency of patient care.

Advanced data and analytics support the prediction of patient outcomes, enabling the allocation and optimization of resources. Wearable medical devices can track various health measurements, and manage and monitor various patient conditions. Mobile Health Applications (mHealth) apps enable patients to manage their healthcare status while communicating with healthcare providers.

AI and machine learning can be applied to improve imagery analysis, drug discovery, and diagnosis. Virtual reality and augmented reality can enhance and better support surgery planning, training, and rehabilitation.

The adoption of new digital technologies in the healthcare industry has brought a rapid increase in the number of smart devices and Internet of Things (IoT) devices. This has also expanded the cyber threat landscape and created a large attack surface that must be managed and controlled. Most healthcare information, security, and network operations teams lack sufficient visibility into their networks, medical devices, and the multitude of IoT devices to quantify risk adequately.

Insider threats continue to put healthcare organizations at risk, as clinicians may inadvertently expose sensitive PHI data while attempting to circumnavigate established policies and governance. In counter-balance, ensuring that clinicians have secure contextual access to the data and technologies they



Threat actor motives for breaches[2]

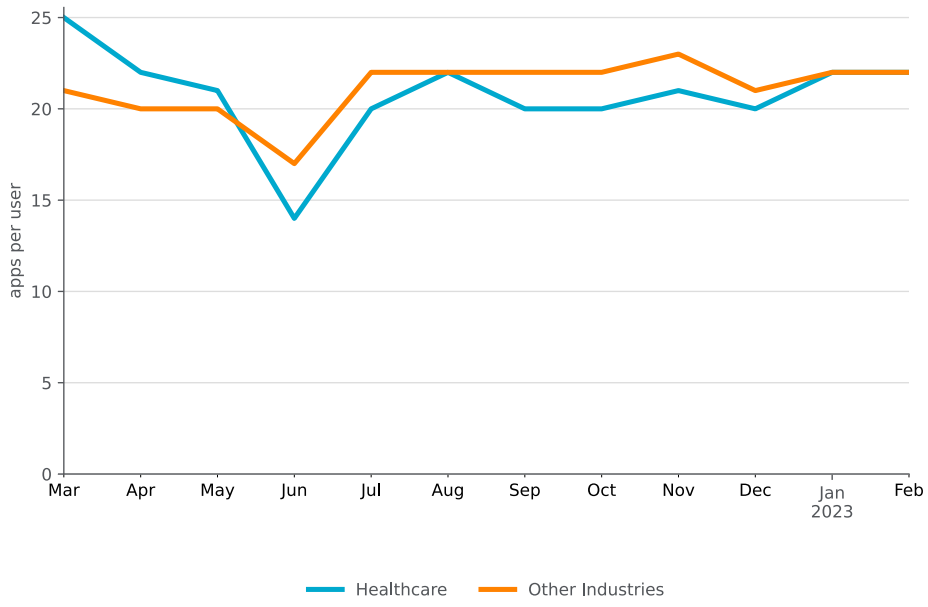
[2] Source: Verizon 2023 Data Breach Investigations Report

need, regardless of their location or device, is essential for timely and high-quality patient care. Secure contextual access to third parties is also a critical issue that must be addressed.

Healthcare organizations remain prime targets for cyber threat actors. Threat actors use a range of techniques, such as phishing and social engineering attacks, malware, and ransomware, to access sensitive data or disrupt operations. In order to help protect the sensitive data, healthcare services require secure data management and encryption to protect data from malicious or inadvertent movement.

Compliance regulations and related governance policies, such as GDPR, POPIA, LGPD, UAE Federal Law No 2 of 2019, and also HIPAA when handling data of U.S. residents or entities, pose significant challenges for IT, security, and network operations teams, as they require mandated operational deliverables for data protection, cybersecurity, risk assessment, and more.

Finally, the user experience must be improved. Some healthcare organizations still rely on legacy MPLS and VPN networks that are expensive, slow to deploy, and create network bottlenecks by backhauling user traffic through corporate data centers.



Average apps per user
Healthcare vs Other Industries - Last 12 months

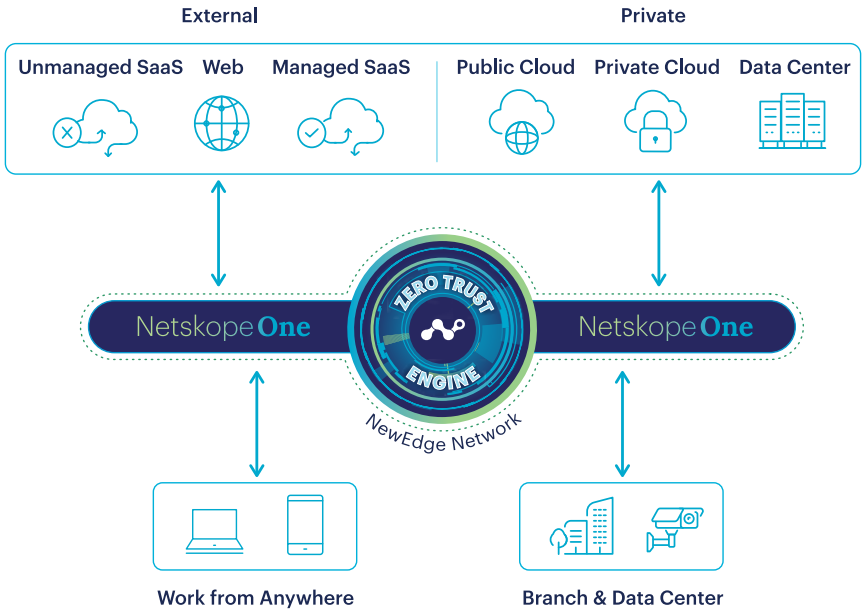
THE NETSKOPE SOLUTION FOR A MODERNIZED HEALTHCARE ENTERPRISE

The Netskope One Platform

The Netskope One unified SASE platform provides optimized access and zero trust security for people, devices, and data anywhere they go, helping organizations reduce risk, accelerate performance, and get unrivaled visibility into any cloud, web, and private application activity. With a data-centric approach to security and performance, Netskope empowers healthcare organizations to tackle evolving threats, manage new risks, adapt to technology changes, accommodate organizational and network shifts, and comply with regulatory requirements.

With Netskope, you can:

- Simplify your security in the cloud with a cloud-native platform that offers converged security and networking services to enable your SASE and zero trust transformation;
- Understand context to better manage risk in order to protect people and data anywhere they go;
- Optimize network connectivity and performance with Borderless SD-WAN;
- Bring security closer to the edge with the Netskope NewEdge network—the world's largest private SASE cloud; and
- Realize better ROI from technology investments.



The Netskope One Platform

IMPORTANT USE CASES BRING VALUE

These example use cases highlight many of the challenges faced by healthcare organizations every day and the Netskope solutions that address them directly.

Use Case #1 - Sensitive Data Loss and Leakage

Scenario:

A clinician may attempt to move sensitive healthcare records, for example X-ray files, outside the sanctioned cloud application through multiple ways. This includes uploading the files to his personal cloud instance, emailing the files to his personal account, copying to a USB memory stick, or even embedding the files in more unstructured formats like images and screenshots. Many existing data protection solutions fail to secure sensitive data across all these exfiltration points. To be truly effective, a zero trust data protection solution needs to monitor the entire business footprint and develop a deep understanding of the business context and risk awareness to enforce the necessary remediation steps.

The Netskope Solution:

Netskope One allows organizations to secure data across all the control points and prevent any accidental or intentional data leakage. The solution includes:

- Web data protection capabilities to prevent sensitive data leakage over untrusted and risky websites.
- Discovery, monitoring, and protection of sensitive data across corporate SaaS applications, including Microsoft 365, Salesforce, Google Workspace, and Slack, and IaaS clouds, including AWS, Azure, and Google Cloud.
- Securely enabling the use of generative AI across organizations with the widest visibility and classification of GenAI apps through ML-assisted discovery and risk assessment. With enforcement measures to stop sensitive data uploads and coaching to educate users on security policies, reducing risky behavior.
- Real-time inspection of all cloud traffic using the Netskope Zero Trust Engine, decoding rich, contextual details about the user, group, activity, location, app, or app instance, including sanctioned and unsanctioned cloud instances to secure sensitive data transactions.
- Extensive DLP protection for email including Microsoft 365 and Gmail via APIs, real-time email protection inline, and even data protection through personal email instances.
- A lightweight Endpoint DLP solution for protecting sensitive data in-use through employees' endpoints and preventing data exfiltration via USB, even when the device is offline.
- Advanced DLP capabilities including file fingerprinting, EDM, OCR, and ML-based classification.

Benefits Delivered:

Comprehensive data protection coverage for securing sensitive data across every network, cloud, endpoint, email service, and user, with the highest degree of data protection efficacy.

Use Case #2 - Collaboration Across Healthcare Organizations

Scenario:

Collaboration across organizations (such as between a university and an affiliated research hospital) is a common area where data ownership and protection conflicts can arise. Typically the organizations sign agreements that outline each party's responsibility for securing protected health information (PHI) data. Many times data collaboration may happen outside the terms of the agreement—without the security or IT team's knowledge. And once proprietary data is exfiltrated from the institution, it can lead to compliance penalties and the possibility of a public data breach. Many solutions fail to assess the risks associated with third-party collaboration and enforce necessary guardrails for protecting data.

The Netskope Solution:

The Netskope One platform, with the Zero Trust Engine at it's core, provides unrivaled visibility and real-time data and threat protection into every cloud, web, and private application activity. The solution includes:

- Deep awareness of context and risk to secure sensitive data with context-aware adaptive access controls. The context includes security postures, dynamic cloud risk scores, user behavior, geolocation, etc.
- Context-driven zero trust access to specific private applications for remote users through Netskope ZTNA Next, while shielding the rest of the applications from discovery and attacks.
- Leveraging multi-data sources and UEBA to determine the user risk posture and enforcing dynamic access controls for the shared documents across the collaboration apps. Restricting the access in case the user risk profile changes or the user device gets compromised, to minimize the risk of data exfiltration.
- Monitoring oversharing of sensitive data in the cloud, preventing insider threats exposing sensitive data accidentally or negligently, blocking data exfiltration to personal accounts to protect highly confidential documents at all costs.

Benefits Delivered:

Benefits to the healthcare organization include a reduction in risk; potential compliance penalties with resulting damage to reputation are avoided. Out-of-policy activities are blocked and prevented from inappropriately using or accessing PHI without relevant controls, which reduces risk for the organization. Secure collaboration has the potential to improve patient outcomes. Collaborating teams can now perform their work and communicate securely to help deliver the best patient outcomes in a timely manner.

> "We have been able to consolidate several solutions we were using into one, Netskope."

Sr. Staff Security Engineer,
Large Enterprise Health Care Providers & Services Company

Use Case #3 - Improving Hospital and Clinic Connectivity and Experience

Scenario:

A leading healthcare network has moved many of its critical applications to the cloud to enable seamless access to internal data to its various clinic and hospital facilities. The deployment of legacy and expensive MPLS has limited the bandwidth for clinic and hospital sites, making it difficult to access cloud operations in a seamless manner to support operations. Further, remote clinicians' traffic was getting backhauled to centralized servers via VPNs, leading to latency and performance issues.

The Netskope Solution:

Netskope One provides secure, reliable connectivity for every site, cloud, remote user, or IoT device so customers can benefit from a truly converged SASE platform that simplifies operations and preserves network performance. The solution includes:

- Netskope Borderless SD-WAN provides every remote user, device, and site with simple, secure, high-performance access to multi-cloud and hybrid-cloud environments.
- Secure and direct access to private applications hosted anywhere through Netskope ZTNA Next, eliminating the need for heavy VPN clients.

Benefits Delivered:

Seamless access to corporate resources from every hospital site, while reducing the costs at the corporate network in the form of MPLS and VPN infrastructure. Simplified traffic steering through Borderless SD-WAN to the Netskope One platform and NewEdge network, delivering security without performance trade-offs and accelerating the adoption of SASE.

> "We experienced a lot of back-and-forth with staff that an organization like ours can never really get ahead of," said the head of IT. "We needed an exact data match. We needed to get an index of existing patients and be able to match it to enforce all the rules. Netskope did this for us—with literally zero false positives."
>
> Head of Information Technology,
> Internationally Recognized Hospital

CUSTOMER SUCCESS STORY

An internationally-recognized hospital partnered with Netskope to enhance data security, overhaul its DLP effectiveness to reach zero false positives, better equip its remote workforce, and achieve the balance of making things easy and secure.

The Challenge

A well-known hospital, renowned for its groundbreaking research, had two significant challenges related to its IT environment and use of cloud applications. The first was to prevent any authorized exfiltration of patient data and do so without causing unnecessary friction, false positives, or security alerts that would slow down its fast-moving staff's ability to collaborate. The second challenge was to prevent malware from entering the hospital network via what the hospital discovered was a wide variety of SaaS apps.

Making its Microsoft 365 implementation secure was a big job compounded by how many hospital team members were linking it to various other applications, including file transfer services such as Dropbox. The hospital didn't have a reliable view of which connections to Dropbox and other apps were benign or potentially exposing data. But it couldn't just shut down those apps, shaky security or not—a too aggressive lockdown against non-sensitive collaboration would have brought staff productivity to a crawl.

The Solution

The hospital's IT team experienced daily escalations over concerns of unauthorized data moving around using insecure apps. Its then-current DLP solution was cross-checking against HIPAA dictionaries—that is, using the healthcare compliance law's definitions as the basis of keywords and other rules—but at best only achieving 70% accuracy, meaning false positives and unnecessary escalation nearly 30% of the time. In-line CASB quickly became a primary need for improving data protection and reducing false positives—specifically a level of visibility and control for thousands of apps (managed and unmanaged), including users, file names, and activity. Implementing Netskope brought an immediate impact.

The Business Benefits

CASB Inline helped the hospital and its heavily distributed staff of caregivers, researchers, and other stakeholders confidently manage and prevent the unintentional or unapproved movement of sensitive data between cloud app instances, with full context of app risk, user risk, and access risk. The hospital was also able to increase the visibility of all of its SaaS apps in use throughout the network, and supplement its existing firewall and other security tools without disruption. The hospital successfully reclaimed countless hours previously spent on manual escalation, chasing down false positives, and forensics.

436

Confirmed data breaches in the healthcare sector with 67% compromising personal data, 54% medical data, and 36% credentials.

+

98%

of threat actor motives are for financial gain, with ransomware often used to target healthcare organizations.

35%

of breaches are perpetrated by trusted and privileged internal users making mistakes, with evidence of collusion with external threat actors.

68%

of breaches in healthcare result from system intrusion, basic web app attacks and miscellaneous errors.

netskope

Source: Verizon 2023 Data Breach Investigations Report

SUMMARY

Netskope helps healthcare organizations improve patient outcomes and reduce costs by safely reaching the full potential of digital transformation. Netskope's capabilities allow healthcare institutions cost-efficient monitoring and enforcement of compliance policies across any mix of digital devices from a single console. Healthcare organizations can securely collaborate while securing patient data, avoiding regulatory fines, and guarding against data breaches.

Netskope, a global SASE leader, helps organizations apply zero trust principles and AI/ML innovations to protect data and defend against cyber threats. Thousands of customers trust Netskope and its powerful NewEdge network to address evolving threats, new risks, technology shifts, organizational and network changes, and new regulatory requirements. Learn how Netskope helps customers be ready for anything on their SASE journey, visit **netskope.com**.