REPORT

Healthcare security trends and the impact of artificial intelligence

April 2025

LUMEN®

Table of contents

Introduction

The healthcare industry has increasingly relied on technology to improve patient care, streamline operations, reduce risk and enhance overall efficiency. Technology once considered shiny and new—like electronic health records (EHRs), telemedicine, and internet of medical things (IoMT) devices—has become almost ubiquitous. This reliance on technology, however, has also made healthcare organizations prime targets for cyber threats. In 2024, healthcare accounted for almost one-quarter (23%) of all data breaches.[1]

It is easy to see why the industry is so highly targeted. Financial gain is the primary motivator behind cyberattacks, and healthcare organizations store vast amounts of sensitive patient data that can be exploited for identity theft, financial fraud or ransomware if it falls into the wrong hands.

Monetary rewards are not the only motivating factor. Some of the largest attacks on healthcare companies have been credited to nation-state actors like China, Russia and Iran who aim to gather intelligence, disrupt infrastructure, or steal trade secrets and technology.[2]

And one of the most troubling reasons why healthcare companies are targets is because of the urgent nature of their operations. Prolonged IT outages can be a matter of life and death, and some of the worst cyber criminals simply do not care.

To complicate matters, the healthcare industry typically has IT infrastructure with numerous connected devices and third-party vendors, which increases the potential attack surface and makes it harder to secure.

In recent years, the integration of artificial intelligence (AI) into healthcare has brought both opportunities and challenges from a cybersecurity perspective. AI has emerged as a powerful tool in healthcare, offering solutions for predictive analytics, personalized medicine and automated administrative tasks. At the same time, the integration of AI has introduced new vulnerabilities and ethical concerns that must be addressed.

In this report we explore the state of cybersecurity and compliance in healthcare, along with the impact of an AI-driven future. By understanding these dynamics, healthcare organizations can be better prepared to avoid and mitigate technology-related risks.

Security trends in healthcare

Below are some of the latest security trends in healthcare – from vulnerabilities, to increasing cyberthreats, rising costs and a fluid regulatory landscape. Later in this report we will dig into some of the ways AI could impact the future of healthcare in the United States.

Vulnerabilities

The healthcare industry has faced many of the same vulnerabilities for several years, but AI is changing the game both for threat actors and cyber defenders.

Phishing/email compromise

While hackers often target unpatched software to breach healthcare networks, more than 90% of cyberattacks on healthcare companies in 2024 involved phishing scams.[3] One recent study revealed the most common initial points of compromise in healthcare security incidents in 2024 were email phishing (63% of respondents), SMS phishing (34%), spear phishing (34%) and email compromise (31%).[4]

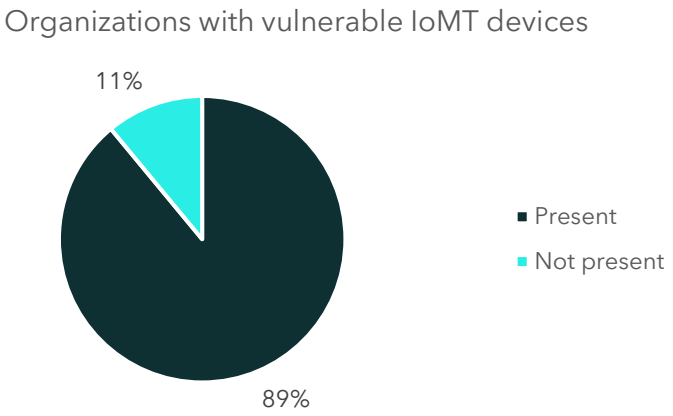
Later in this report we will look at the latest trend that is increasing threat actors' ability to create more sophisticated phishing scams that are harder to detect: artificial intelligence.

Medical devices

The proliferation of IoMT devices has introduced new vulnerabilities, and many of the machines lack basic cybersecurity protections. Infusion pumps, ventilators, and imaging machines can be exploited to disrupt treatments or gain access to broader hospital networks[5] In fact, a recent study found that 89% of healthcare organizations have vulnerable IoMT devices connected to the internet. In addition, 20% of these devices are connected to hospital information systems, and 8% to imaging systems (e.g., x-ray, MRI and CT machines.)[6]

Figure 1

89% of healthcare orgs run IoMT devices that contain vulnerabilities linked to ransomware and are insecurely connected to the internet.[6]



Source: Infosecurity Magazine | March 28, 2025

Insufficient budgets

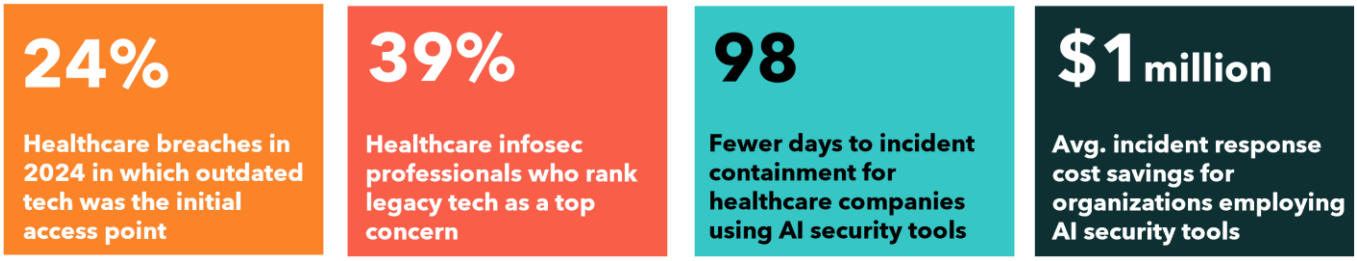
Historically, healthcare organizations have invested 6% or less of their IT budgets in cybersecurity; however, more money is now being spent on security improvements, with 30% of respondents saying they are investing more than 7% of their IT budget on cybersecurity in 2025.[7]

Staffing challenges

Hiring and retaining cybersecurity employees has been a persistent problem across industries for many years. In healthcare, 53% of organizations report being challenged by a lack of in-house cybersecurity expertise. While 30% of these companies report being understaffed or severely so, and only 14% of healthcare companies say their IT security teams are fully staffed.[8]

Legacy systems

Outdated IT equipment, including legacy operating systems or unsupported software, was the initial access point in 24% of the most severe security incidents in the healthcare industry in 2024. In addition, nearly half of the respondents in one recent study said more than 10% of their infrastructure included legacy systems. Because of these issues, it's no surprise that legacy technology ranks as a top cybersecurity concern for 39% of cybersecurity professionals in the healthcare industry.[8]



Source: Dialog Health | January 2025

Increasing cyber threats

As healthcare companies seek to mitigate the above-listed vulnerabilities, threat actors continually look for opportunities to launch catastrophic attacks and steal data. Some of the most common types of attacks on the healthcare industry include:

Ransomware

Ransomware continues to be one of the most pervasive threats for healthcare companies, and statistics are trending in the wrong direction. For example, the U.S. Department of Health and Human Services (HHS) reported a 264% surge in healthcare-targeting ransomware incidents over the past five years.[9] In addition, five of the 10 largest ransomware attacks in 2024 targeted healthcare companies.

Supply chain attacks

According to one recent study from the Ponemon Institute, the types of attacks most likely to impact patient care are those that target the supply chain. In addition, 68% of healthcare IT leaders say their organization experienced a supply-chain in 2024, and 82% of those attacks disrupted patient care.[10]

Cloud/account compromise

The Ponemon study also revealed that the most frequent attacks in healthcare are against the cloud, with 69% of respondents saying their organizations experienced an average of 20 cloud/account compromises in the past two years.

Cost of being breached

The cost of data breaches continues to be a serious issue for healthcare companies. In fact, the healthcare industry has experienced the highest data breach costs of all industries for 13 consecutive years, and the average cost of a breach hit $10.93 million – a jump of more than 53% since 2020.[11]

Notably, hospitals are attractive targets for cybercriminals due to the pressure these organizations face to quickly restore critical systems and data required for patient care. In addition, the theft of valuable protected health information (PHI) is a growing concern, with more than half of healthcare CFOs (51%) saying privacy breaches were a bigger risk in 2024 than in 2023.[12]

Regulatory changes impacting healthcare IT

Elections can alter the healthcare landscape as each new administration seeks to implement its own policies and priorities. Whereas one administration might want to expand public healthcare programs or introduce new privacy regulations, the next could promote private-sector solutions and deregulation. These shifts can lead to changes that affect how healthcare providers operate and how patients access care.

Impact on healthcare companies

Although the elements of this EO will be implemented over time, many organizations within the healthcare sector are considered "critical infrastructure" and will likely be impacted one way or another. For this reason, healthcare IT leaders should begin thinking about potential impacts.

For example, healthcare providers might need to work more closely with state and local governments to align their infrastructure and preparedness plans with the new national resilience strategy. In addition, as current regulations and policies are reviewed and revised, potential updates could require changes in preparedness, manufacturing practices, data security and reporting. Staying compliant could be crucial for some healthcare companies' continued operation and funding.

In addition to the myriad of existing healthcare-related regulations, healthcare companies should be aware of an executive order (EO) signed on March 19, 2025, that could impact the industry. The "Achieving Efficiency Through State and Local Preparedness" EO changes the way the United States prepares for and responds to a variety of risks, including cyber attacks, by stating that preparedness will be "owned and managed on a state, local and individual level." The order also calls for the development of a national resilience strategy, prioritizes a "risk-informed approach" for approving and funding critical infrastructure projects, and orders the review and potential revision of current infrastructure policies.

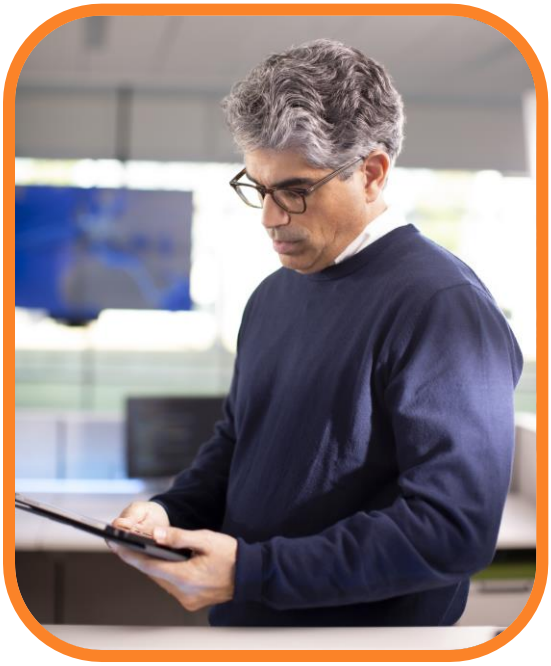
Artificial intelligence

Artificial intelligence and machine learning are the newest trends impacting security in the healthcare industry. They are being integrated into chatbots, patient rooms, diagnostic testing, research studies and more – all to improve innovation, discovery and patient care.[13]

Given the three issues outlined above – ongoing vulnerabilities in healthcare IT, the continued rise of cyber threats, and regulatory changes – it's important to look at the impact that artificial intelligence has on the healthcare industry.

Benefits of AI in healthcare

Some of the benefits we're already seeing from the use of AI in healthcare include:



- **Improved diagnostics:** AI enhances diagnostic accuracy by analyzing medical images and data more efficiently than traditional methods. This leads to quicker and more accurate diagnoses.
- **Personalized medicine:** AI enables personalized treatment plans by analyzing patient data to predict the most effective treatments. This approach helps improve patient outcomes and reduce trial-and-error in treatment
- **Predictive analytics:** AI uses predictive analytics to identify potential health risks and vulnerabilities before they become critical. This proactive approach helps with early intervention and prevention.
- **Streamlined administrative tasks:** AI can automate administrative tasks such as scheduling, billing, and record-keeping, which can free up healthcare professionals to focus more on patient care.
- **Enhanced patient care:** AI-driven tools like virtual assistants and chatbots improve access to care, especially for patients in rural or underserved areas. These tools can provide basic healthcare information, schedule appointments, and offer next-step guidance.
- **Drug discovery and development:** AI could accelerate the drug discovery process by analyzing vast datasets to identify potential drug candidates and predict their effectiveness. This could lead to faster development of new treatments.
- **Operational efficiency:** AI helps improve operational efficiency by optimizing resource allocation, reducing wait times, and enhancing overall workflow in healthcare facilities.

The role of AI in healthcare security

As healthcare organizations implement AI to innovate, discover new drugs, and improve efficiency and patient care, threat actors are weaponizing AI to create highly targeted campaigns. Healthcare companies, in turn, are using AI-driven security solutions to help stop attacks before they occur.

AI-driven attacks

Although AI became a mainstream topic just a few years ago, elements of the technology have been around for decades. Threat actors are already adopting advanced AI and machine learning-based tactics to launch sophisticated attacks, and some experts believe the trend is only going to increase.[14] In fact, Gartner predicts that by 2027, 17% of all cyberattacks will involve GenAI.[15]

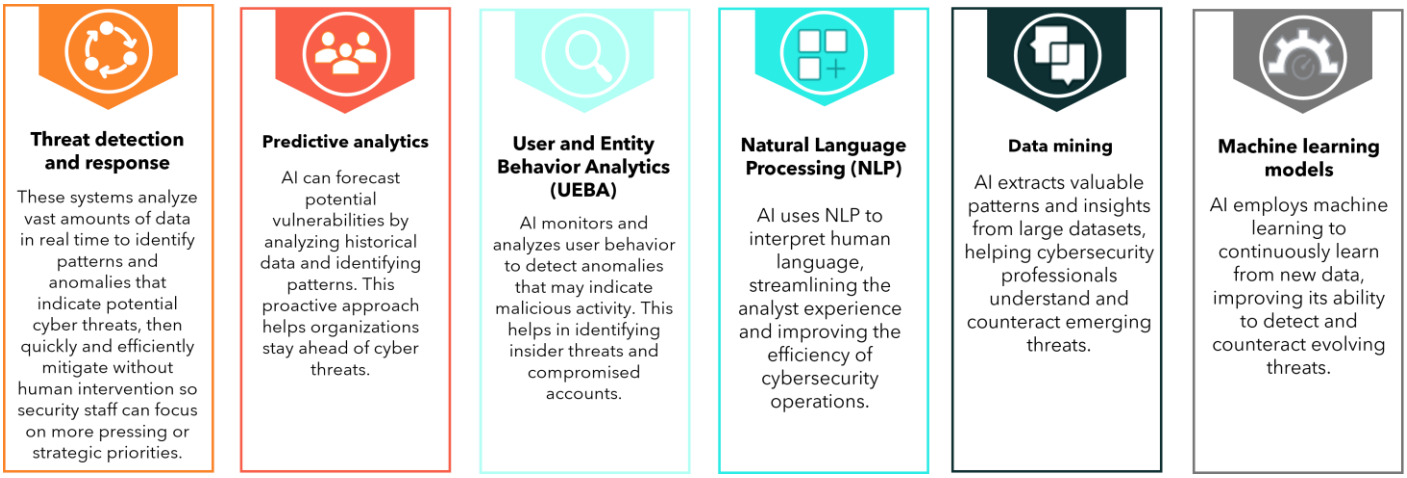
Some of the AI-driven tactics cybercriminals use today include:

- Sophisticated phishing attacks: AI can craft highly convincing phishing emails that lack common red flags, making them harder for employees to detect.
- Targeted spear phishing: Threat actors use AI to analyze stolen data to create personalized spear-phishing emails, increasing the likelihood of successful attacks.
- Automated data analysis: AI tools can quickly process and organize large amounts of stolen data, aiding cybercriminals in identifying valuable targets.
- Accelerated brute force attacks: AI can accelerate brute-force password cracking, allowing even quicker access to systems.
- System vulnerability analysis: Threat actors have used AI to identify and exploit vulnerabilities, making the attacks more efficient and damaging.

In fact, healthcare companies have already fallen victim to attacks involving AI. The worst of these happened in February 2024 when Change Healthcare experienced one of the largest cybersecurity breaches in healthcare history. Research later determined every tactic listed above was used in the ransomware attack that affected approximately 190 million individuals.[16]

AI-driven security solutions

Because cybersecurity seems to be a never-ending game of Whac-A-Mole™ between threat actors and defenders, the industry has developed AI-driven security solutions to combat the attackers' tactics. Some of these include:



Recommendations for IT security in healthcare

Given the vulnerabilities, threats, regulatory changes and AI-powered attacks impacting the healthcare industry, immediate, proactive steps are necessary to mitigate overall risk.

Strengthen cybersecurity posture

Investing in advanced, AI-driven security tools is essential. AI-backed cybersecurity technologies can protect sensitive patient data by quickly identifying fraud and blocking bad actors, thereby maintaining safe experiences and building trust between healthcare companies and their stakeholders.

In addition, real-time data processing requires faster speeds to offer timely diagnostics and personalized treatment recommendations as patients receive care. This is why edge solutions integrated with AI can enhance healthcare operations and patient care by keeping data close to the source and reducing latency.

Finally, regular audits and penetration testing are crucial to identify and address vulnerabilities, helping ensure that healthcare organizations remain resilient and manage risks.

Enhance regulatory compliance

The number of mandatory regulations and voluntary standards a healthcare organization may have to comply with – and the volume of changes that might occur as a result – can increase the potential for compliance failures.[17] Three strategies for mitigating this risk include:

Adopt voluntary standards: Voluntary healthcare standards most often exceed the healthcare regulatory compliance requirements to better protect patients, healthcare data, or members of the workforce. Examples of technology-related voluntary standards include ISO 27001, ISO 27799, HL7 and the NIST framework.

Consider compliance software: To mitigate the risk of being swamped by regulations and standards, or overlooking a critical implementation specification, healthcare organizations should evaluate customizable healthcare regulatory compliance software. These solutions can be used to determine when one standard conflicts with or duplicates another, or when a state regulation partly exempts an organization from compliance.

Partner with an expert. A trusted technology partner can help you meet and exceed regulations by conducting assessments and helping you implement compliant solutions. Lumen provides a detailed gap analysis based on regulatory and compliance standards, along with a roadmap to meet or exceed regulatory standards. This includes compliance assessments, program development, and readiness assessments for various standards such as HIPAA, NIST CSF, and FISMA

Foster a culture of security

A culture of security helps ensure that all stakeholders are aware of and actively engaged in protecting patient data. Continually training staff about cybersecurity best practices and encouraging collaboration between IT and healthcare professionals can significantly enhance the security posture of the organization. Healthcare organizations should implement AI- and cloud-ready technologies to support scalable and secure data management.

Prepare your network

As we have seen, AI is transforming healthcare in profound ways. But an AI-enabled future requires preparation, and healthcare companies must ensure their networks can handle the increased data demands as more and more AI solutions are brought online. This is because AI applications process vast amounts of data in real-time, which can quickly overwhelm outdated systems and cause them to struggle to efficiently process and store data. The subsequent delays and operational errors can lead to financial loss and poor patient outcomes. Additionally, treliance on legacy infrastructure can expose critical weaknesses, which makes it easier for cyber attackers to exploit vulnerabilities and gain unauthorized access to sensitive information.

Upgrading to modern, secure systems is essential to be able to effectively handle the data-intensive requirements of AI technologies. Without modernized network infrastructure, healthcare organizations risk data bottlenecks, delays in critical diagnostics, and potentially compromised patient care.

By upgrading their networks, healthcare companies can help ensure seamless data flow, which can improve patient outcomes while helping decrease costs and minimize risks.

Utilize managed and professional services

Managed and professional services can play a crucial role in helping healthcare companies prepare for the AI future and beyond. Some of the key ways an IT partner can help you in your AI journey include:

- **Identifying impactful AI applications**: Managed and professional services can help healthcare organizations identify the most impactful AI applications for their specific needs. This includes understanding how AI can improve diagnostics, provide personalized medicine, utilize predictive analytics and streamline administrative tasks.
- **Seamless integration with existing systems**: The right partner can help ensure that AI technologies are seamlessly integrated with your existing systems, which helps avoid disruptions and helps ensure that AI tools work effectively alongside current infrastructure.
- **Ongoing maintenance and optimization:** Managed services provide ongoing maintenance and optimization of AI systems. This helps ensure that AI tools remain up-to-date and continue to deliver value over time.
- **Staff training:** Professional services can offer training to healthcare staff on how to use AI tools effectively. This helps ensure that employees are comfortable with new technologies and can leverage them to improve patient care.
- **Regulatory compliance:** Managed services can assist healthcare organizations in staying compliant with evolving regulations by conducting assessments, developing compliance programs, and providing readiness assessments for various standards.

By leveraging managed and professional services, healthcare companies can effectively prepare for an AI-enabled future, enabling them to harness the benefits of AI while minimizing risks and maintaining compliance.

How Lumen can help

Networking and security solutions

With the integration of AI into healthcare, the demand for high-capacity, low-latency networks has never been greater. Lumen networking solutions are designed to support healthcare companies as they prepare for this AI-enabled future. Our robust infrastructure, including our extensive fiber network and advanced AI-driven security solutions, enables healthcare organizations to leverage AI technologies to enhance patient care, streamline operations, and help improve diagnostic accuracy.

Lumen provides the following networking and security solutions:

- **Control network connectivity:** Lumen® Network-as-a-Service (NaaS) provides real-time, self-service, scalable control over network connectivity, enabling businesses to manage, bandwidth, path, and latency dynamically.
- **Optimize costs, minimize downtime and enhance customer experiences:** Lumen® DDoS Mitigation services provide comprehensive protection against DDoS attacks by rapidly filtering malicious traffic and returning clean traffic to customers, leveraging a multi-layered scrubbing architecture and advanced threat intelligence from Black Lotus Labs.
- **Minimize risk:** Lumen Defender℠ powered by Black Lotus Labs® offers proactive network protection by automatically blocking traffic from risky sources before it breaches internal networks, leveraging comprehensive threat intelligence.
- **Simplify networking and security:** Lumen® SASE Solutions unify network and security management through a centralized, cloud-based experience, simplifying the design, purchase, deployment, and orchestration of software-defined network infrastructure and information security.
- **Minimize costs and scale on your terms:** Lumen® SD-WAN solutions support secure, scalable, and cost-efficient deployment and management of hybrid networks, providing complete visibility, control, and security across various connectivity types.
- **Optimize efficiency for customers and employees:** Rapid Threat Defense integrates Black Lotus Labs intelligence to proactively block known malicious traffic, enhancing operational efficiency and reducing the burden on IT staff.
- **Focus resources, minimize expenses:** Lumen Security Operations Center as a Service (SOCaaS) offers fully managed cybersecurity threat detection, incident management, and response support, providing visibility across an agency into cyber activity.
- **Reduce costs and risks:** Lumen Incident Reporting system provides prompt reporting and management of risk-related incidents involving company employees, vehicles, and facilities, facilitating rapid response and resolution.
- **Reduce workloads while defending critical apps and data:** Lumen's managed and professional security solutions provide comprehensive protection through proactive threat monitoring, incident response, penetration testing and tailored advisory services, providing robust security and compliance for businesses.

BLACK LOTUS LABS® by Lumen

Black Lotus Labs® is the award-winning, in-house threat research arm of Lumen. The team of data scientists, reverse engineers, security engineers, and threat analysts leverages their unmatched visibility into the Lumen network to protect businesses and help keep the internet clean.

Black Lotus Labs use advanced threat technology to identify and eliminate threats quickly, employing machine learning algorithms to automate protection and neutralize threats. The team has been involved in the identification and takedown of some of the most high-profile malware of the past decade.

By providing secure, high-speed connectivity and real-time data processing capabilities, Lumen helps to enable healthcare providers to implement AI applications such as predictive analytics, personalized medicine, and automated administrative tasks. This helps improve patient outcomes, minimize security and compliance risks, reduce costs and increase revenue.

> Lumen has won three consecutive Cybersecurity Breakthrough Awards including the 2022 Network Security Provider of the Year award, the 2023 SASE Solution of the Year award, and the 2024 Threat Intelligence Company of the Year award.

The bottom line

The integration of AI into healthcare presents both opportunities and challenges in the realm of cybersecurity. By understanding current security trends, vulnerabilities, regulatory changes and the impact of AI, healthcare organizations can better prepare for and mitigate cyber threats. Implementing robust security measures, staying updated with regulations, and fostering a culture of security are essential steps in safeguarding patient data and ensuring the continued advancement of healthcare technology.

Your network infrastructure is the cornerstone of your AI efforts

The Lumen network supports the dynamic demands of AI-powered technologies and enhances patient care by providing high-capacity connections, deep IP peering and AIOps to leverage AI/ML apps without the constraints of a traditional network.

View security solutions

Footnotes

[1] Healthcare Was the Most Breached Industry in 2024 | HIPAA Journal | February 2025
[2] Hacking and Healing: Nation-States, Cyber Attacks, and Healthcare Law | Leech Tishman | April 2024
[3] 120+ Latest Healthcare Cybersecurity Statistics for 2025 | Dialog Health | January 2025
[4] Survey Confirms Majority of Healthcare Orgs Plan to Increase Cybersecurity Investment | HIPAA Journal | March 2025
[5] Healthcare's AI-Powered Cyber War-What Security Leaders Must Do Now | Healthcare Business Today | March 2025
[6] Nine in Ten Healthcare Organizations Use the Most Vulnerable IoT Devices | Infosecurity Magazine | March 28, 2025
[7] Survey Confirms Majority of Healthcare Orgs Plan to Increase Cybersecurity Investment | HIPAA Journal | March 2025
[8] 120+ Latest Healthcare Cybersecurity Statistics for 2025 | Dialog Health | January 2025
[9] Rise in Healthcare Data Breaches & the Impact for Healthcare Providers in 2024 | Bradley | March 2024
[10] 2024 Ponemon Healthcare Cybersecurity Report | Ponemon Institute | October 2024
[11] Cost of a Data Breach Report 2024 | IBM | 2024
[12] Healthcare Security in 2024: The Cyberthreat Landscape | BDO | April 2024
[13] How AI Is Being Used to Benefit Your Healthcare | Cleveland Clinic | September 2024
[14] Editorial: Why AI Will Increase Healthcare Data Breaches | HIPAA Journal | October 202
[15] Gartner Forecasts Global Information Security Spending to Grow 15% in 2025 | Gartner | August 2024
[16] A year since the Change Healthcare breach, what have we learned? | Healthcare IT News | February 2025
[17] What is Healthcare Regulatory Compliance? | HIPAA Journal | January 2025

Why Lumen?

Lumen is your single provider to enable digital transformation. With a comprehensive portfolio and experienced talent, we can help safeguard your customer experience, protect your confidential data, and manage threats. Backed by the extensive and deeply peered Lumen global network, Black Lotus Labs® threat intelligence, and our skilled and experienced team of security experts, Lumen is a trusted partner to help improve your security posture.

866-352-0291 | lumen.com | info@lumen.com

LUMEN®