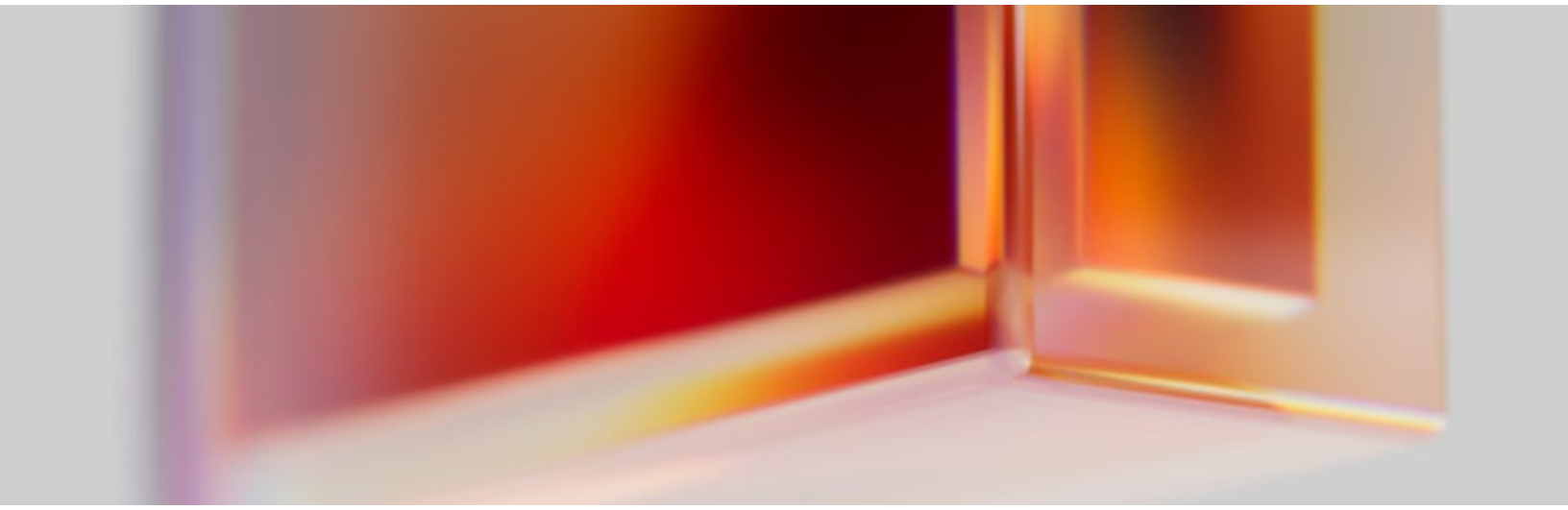


EXECUTIVE BRIEF

The Transformative Challenges and Complexity of Securing Healthcare

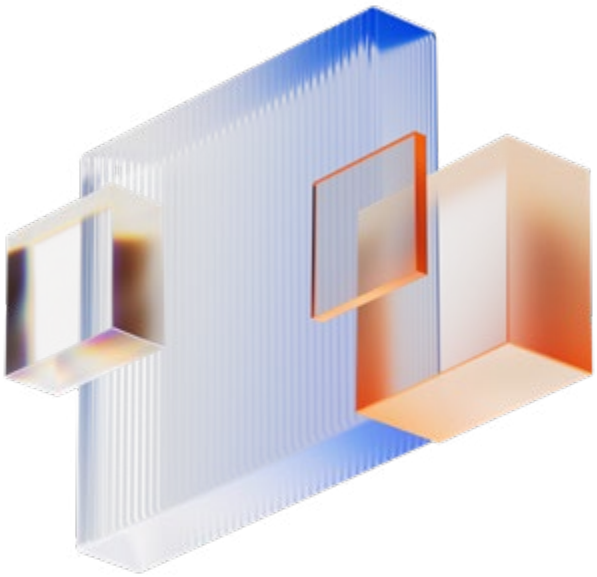
Four critical cybersecurity issues affecting healthcare today.

The healthcare sector is among one of the most increasingly vulnerable sectors to cyber threats, posing significant risks to patient safety, data confidentiality, and operational integrity. The stakes have also never been higher in healthcare, with the world recovering from the impacts of the COVID-19 pandemic, new medical technologies and applications affecting the wellness and safety of patients throughout their lifetime. This brief outlines the transformative challenges in healthcare cybersecurity and identifies the top four critical issues currently affecting the sector.

What's at Risk?

While the financial and monetary impacts from cyberattacks on hospitals, insurance providers, and other key components of the healthcare sector have become increasingly frequent headlines, it's poses even greater risks on cornerstone of healthcare: patient care and outcomes. The cascading effects of successful cyberattacks on critical healthcare infrastructures and electronic health records (EHR) can disrupt patient care in some frightening ways:

- Patients don't get the care they need when healthcare providers are taken offline due to ransomware or DDoS attack.
- Surgeons postpone surgeries because the information necessary to perform a life-saving surgery becomes inaccessible.
- Failures in diagnostic procedures and laboratory tests result in delayed medical treatment.
- Emergency Room (ER) bypass causes ambulances to diverge to healthcare facilities miles farther, leading to degraded and irreversible outcomes.



Transformative Challenges in Healthcare Cybersecurity

1. Integration of Internet of Things (IoT) Devices: Although innovations in the health technology space has led to the adoption of IoT devices in healthcare, such as smart monitors and connected medical equipment, it has simultaneously expanded the attack surface. Many of these devices lack robust security features, making them susceptible to unauthorized access and control that could lead to further malicious network access.
2. Electronic Health Record (EHR) Systems: The digitization of patient records has streamlined information sharing but also centralized sensitive data like personal identifiable information (PII), making EHR systems prime targets for cyberattacks. Ensuring the security of these systems is paramount to protect patient confidentiality.
3. Remote Work and Telehealth Services: The rise of telehealth and remote work arrangements has introduced new vulnerabilities. Insecure home networks and personal devices used by healthcare professionals can become entry points for cyber threats.
4. Third-Party Vendor Dependencies: Healthcare organizations often rely on third-party vendors for services like billing and data management. Security breaches within these external entities can compromise the healthcare provider's systems and data.

Four Critical Cybersecurity Issues Affecting Healthcare Today

As illustrated above, these changes in the healthcare industry have given rise to and contributed to several critical cybersecurity issues. Below are some of the most pressing issues affecting healthcare today and what their impacts are.

1. Ransomware Attacks

Description: Ransomware consists of malicious software that encrypts confidential healthcare data, with attackers demanding payment for decryption keys and threatening to sell data on black markets. These attacks often lead to hefty payments, negative impacts on patient care due to downtime, and encourage bad actors to engage in even more ransomware attacks.

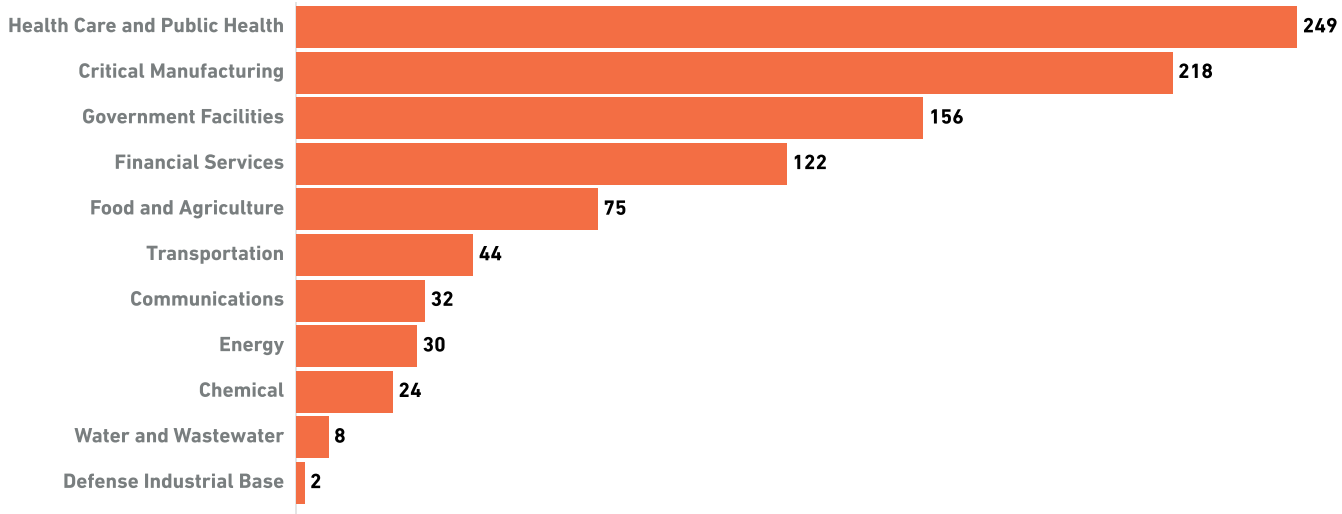
Impact:

- In 2023, the healthcare sector filed the greatest number of ransomware complaints with the FBI (Figure 1).[1]
- A 2024 survey revealed that 67% of healthcare organizations experienced a ransomware attack in the past year.[2]

Figure 1

Critical Infrastructure Sectors Impacted by Ransomware in 2023

Number of organizations filing ransomware complaints with the FBI, by sector



Source: FBI Internet Crime Report 2023

2. Phishing and Social Engineering Attacks

Description: Phishing and social engineering attacks involve deceptive communications trick healthcare staff into revealing sensitive information or granting system access.

Impact:

- In 2021, phishing was the initial attack vector in 40% of cyberattacks, marking a 33% increase from the previous year.[3]
- In 2024, 88% of healthcare workers opened phishing emails, highlighting the sector's vulnerability to such attacks.[4]

3. Data Breaches

Description: Data breaches are caused by unauthorized access to confidential patient information due to hacking, insider threats, or inadequate security practices.

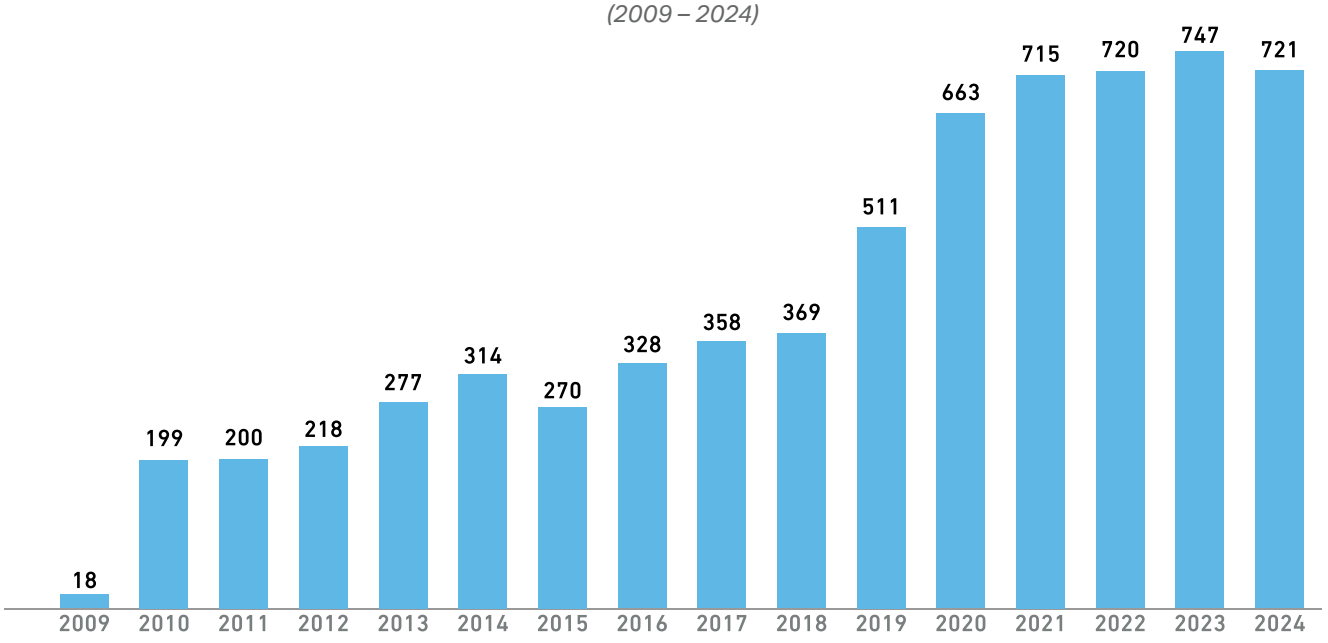
Impact:

- Since the COVID-19 pandemic, healthcare data breaches of 500+ records have reached record highs (Figure 2).[5]
- In 2023, 79.7% of healthcare data breaches were attributed to hacking incidents, up from 49% in 2019.[5]

Figure 2

Healthcare Data Breaches of 500+ Records

(2009 – 2024)



Source: HIPAA Journal

4. Insider Threats

Description: Insider threats involve security breaches originating from within the organization, either maliciously or inadvertently. Due to the rise of third-party vendor dependencies, insider threats have expanded the number of people who have access to sensitive data and systems within a healthcare organization.

Impact:

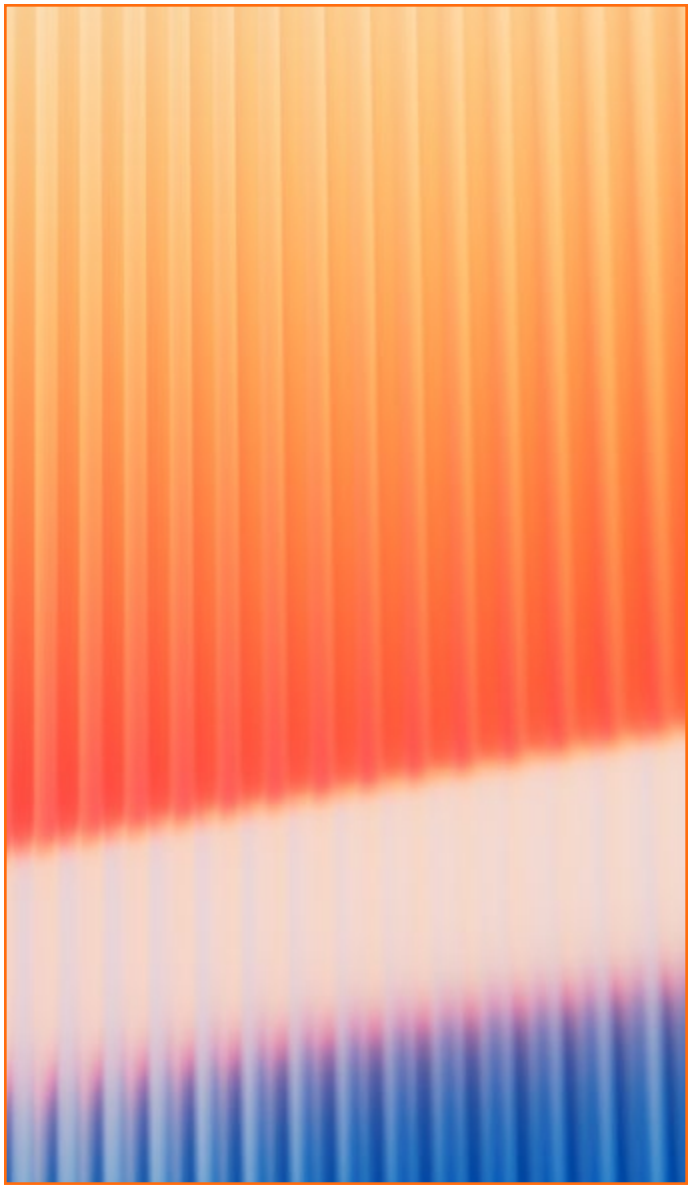
- In 2024, insider threats accounted for 22% of all healthcare cybersecurity incidents.[6]
- Approximately 26% of human factor-based breaches in healthcare result from insider carelessness, negligence, or apathy.[7]

Conclusion

Looking forward, the healthcare sector remains one of the most vulnerable sectors to cyberattacks. To safeguard patient data, maintain trust, and ensure uninterrupted service delivery, healthcare organizations must have the cybersecurity services, solutions, and expertise to be adequately prepared.

Addressing these challenges can sound overwhelming and complex. SonicWall's cutting-edge cybersecurity solutions are tailored to help healthcare organizations confront these challenges effectively. With features like advanced threat detection, real-time ransomware prevention, secure access for remote workers, and integrated network security solutions, SonicWall provides the tools healthcare organizations need to protect sensitive data, mitigate insider threats, and maintain compliance with industry regulations. Leverage SonicWall's expertise and robust security offerings so healthcare organizations can stay ahead of cyber threats and focus on what they do best: caring for patients.

Learn more in SonicWall's latest threat brief on healthcare or contact us.



[1] FBI Internet Crime Complaint Center

[2] Microsoft

[3] HIPAA Journal

[4] Varonis

[5] HIPAA Journal

[6] Verizon

[7] Perspectives in Health Information Management

About SonicWall

SonicWall is a cybersecurity forerunner with more than 30 years of expertise and a relentless focus on its partners. With the ability to build, scale and manage security across the cloud, hybrid and traditional environments in real time, SonicWall can quickly and economically provide purpose-built security solutions to any organization around the world. Based on data from its own threat research center, SonicWall delivers seamless protection against the most evasive cyberattacks and supplies actionable threat intelligence to partners, customers and the cybersecurity community.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

© 2025 SonicWall Inc. ALL RIGHTS RESERVED.
SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. Except as set forth in the terms and conditions as specified in the license agreement for this product, SonicWall and/or its affiliates assume no liability whatsoever and disclaims any express, implied or statutory warranty relating to its products including, but not limited to, the implied warranty of merchantability, fitness for a particular purpose, or non- infringement. In no event shall SonicWall and/or its affiliates be liable for any direct, indirect, consequential, punitive, special or incidental damages (including, without limitation, damages for loss of profits, business interruption or loss of information) arising out of the use or inability to use this document, even if SonicWall and/or its affiliates have been advised of the possibility of such damages. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.