Cyber Risk Benchmark

Trend Report for Healthcare Vulnerability Management

The Ups and Downs of Vulnerability Management Across Healthcare Segments

Clearwater

2025 Report

Report Contents

Executive Introduction 3

Healthcare Segments under Review 3

- Healthcare Software, Analytics, and Business Services 3
- Physician, Dental, and Specialty Practice Clinics 3
- Healthcare Centers and Surgical Hospitals 3

Asset Growth and Vulnerability Findings 4

Average Vulnerabilities per Asset for Healthcare 4

Average Vulnerabilities per Asset by Segment 5

Average Critical Vulnerabilities per Asset for Healthcare 6

Average Critical Vulnerabilities per Asset by Segment 7

Recommendations 9

Executive Introduction

Without exception, vulnerability management continues to grow in complexity across those that provide healthcare to patients and those supporting care delivery and management through specialized technology and business services. With one of the most complex, interconnected technology landscapes and the critical business constraints that require a cautious approach to vulnerability remediation to not disrupt patient care or vital services, vulnerability management in healthcare is an increasingly challenging task.

Healthcare environments create a vast attack surface that requires constant risk management. Cyberattacks targeting sensitive health data, aiming to disrupt patient care or infiltrate a healthcare supply chain, rely on vulnerability exposures to facilitate their tactics. Security leaders in healthcare are keen to know where they stand as compared to like organizations when it comes to vulnerability management, whether it is performed in-house or with a managed security service provider (MSSP).

Clearwater's Benchmark Report on Vulnerability Management aims to fill that void. Derived from the data within our Security Operations Center (SOC) and managed security platform, the report looks at trends across Clearwater's large universe of healthcare clients. Our goal is to help elevate vulnerability risk management across the industry and provide data-driven insight to organizations so they can improve their cybersecurity programs.

Healthcare Segments under Review

In this report, we break out the data and look at vulnerability specifics from the following healthcare segments:

Healthcare Software, Analytics, and Business Services

These companies provide services, specialized software, and analytics platforms supporting healthcare providers.

Physician, Dental, and Specialty Practice Clinics

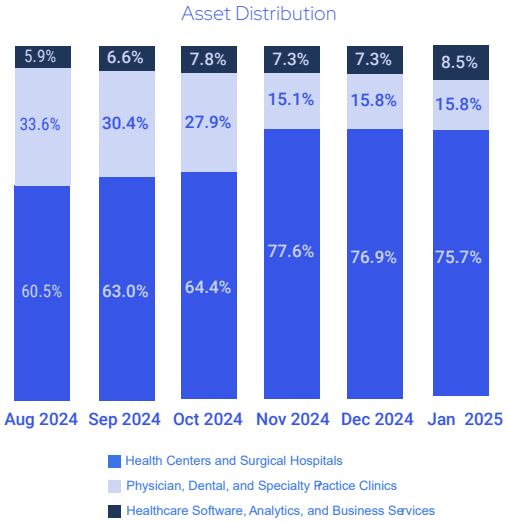
Small to large practice groups that provide healthcare services or specialized healthcare.

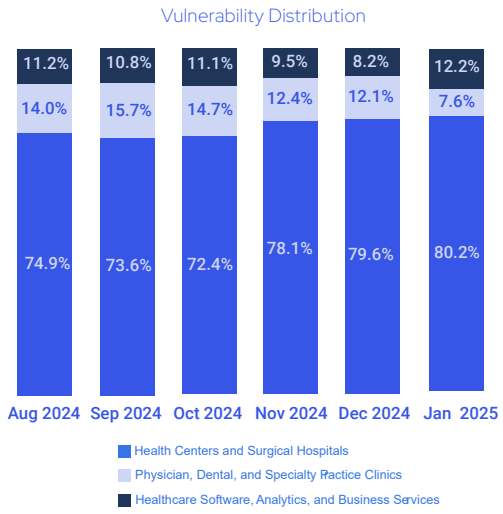
Healthcare Centers and Surgical Hospitals

This group encompasses the hospitals and healthcare centers, including rural and critical access hospitals.

Asset Growth and Vulnerability Findings

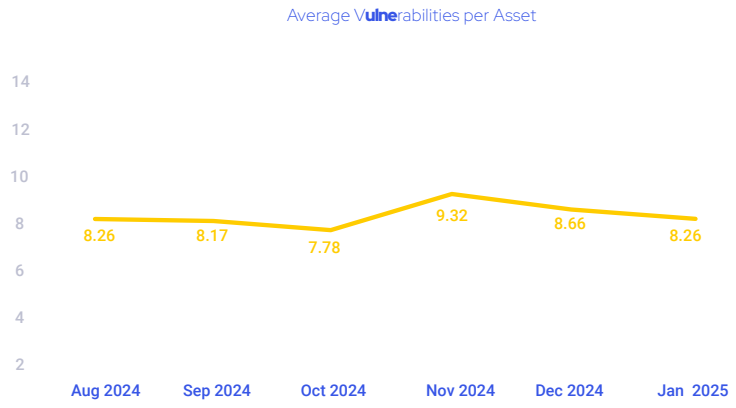
As our client base grows, so does the base of assets that Clearwater provides vulnerability scanning and tech-enabled managed services. The data shared in this report spans August 2024 to January 2025.





Looking at the asset distribution compared to the vulnerability distribution over the six month period, it is clear that the growth in vulnerabilities varies across the segments. The increase in the number of assets would align to the growth in identified vulnerabilities if the growth in assets and the count of vulnerabilities on these systems were similar. In August 2024, Health Centers and Surgical Hospitals had nearly 75% of all the vulnerabilities for that month, yet the total assets were slightly over 60%. This segment in January 2025 does even out, but Physician, Dental and Speciality Practice Clinics and Healthcare Software, Analytics, and Business Services show how their segments shift in vulnerabilities as compared to the number of assets.

Average Vulnerabilities per Asset for Healthcare

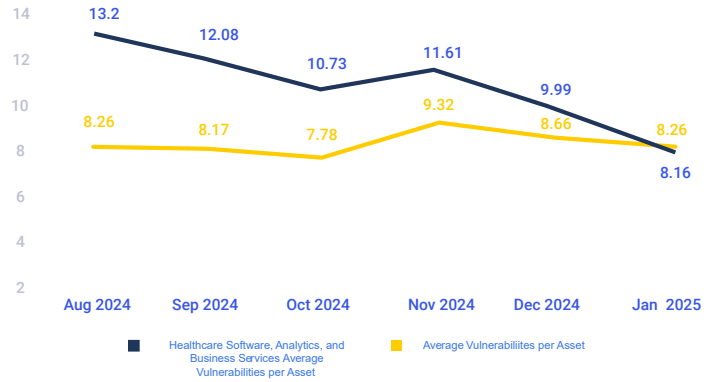


The average number of vulnerabilities per asset also fluctuates. In this report, the average is getting better in October, then spiking to the highest level of 9.32 per asset in November 2024 before trending back downward.

Average Vulnerabilities per Asset by Segment

Looking at the specific segments and their respective average vulnerabilities per asset shows some vulnerability management problems unique to each segment.

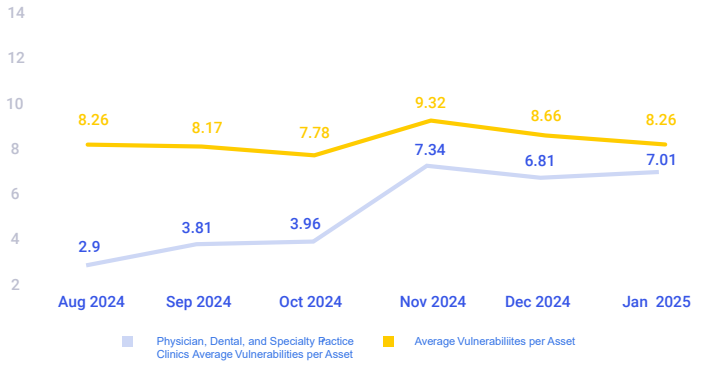
Healthcare Software, Analytics, and Business Services



One of the surprising points we found was that the Healthcare Software, Analytics, and Business Services segment started with the highest number of vulnerabilities per asset compared to the average across all segments. These companies generally have more agility to pick and grow their environments and manage vulnerabilities with fewer constraints as they don't have to worry about disrupting patient care directly. Most of these companies would be considered part of the healthcare supply chain, and this data highlights the risk variability across the segment. In January, the segment dipped below the overall average, showing how diligently this segment can make quick improvements. This is partly because they have a lower asset count to manage, and we noted that their security and IT teams could react faster to vulnerability findings and remediation prioritization than those in other segments.

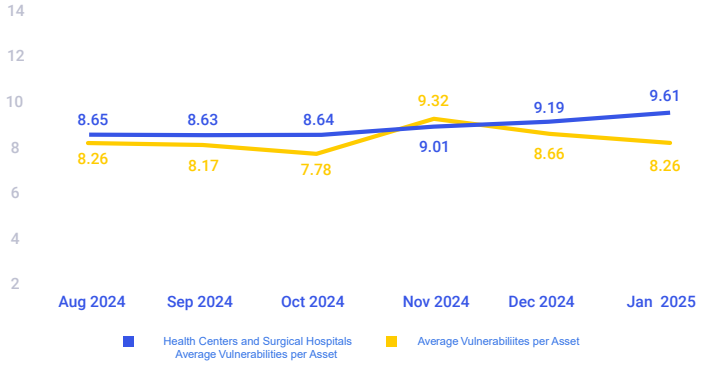
Physician, Dental, and Specialty Practice Clinics

Physician, Dental, and Specialty Practice Clinics' has been the best performing segment in terms number of vulnerabilities per asset, but the number has trended upward significantly in the second half of the six-month review period. There has been movement up and down, and as of January, this segment is still below average and is dealing with more than double the number of vulnerabilities per asset as in August 2024.



Healthcare Centers and Surgical Hospitals

The Health Centers and Surgical Hospitals segment has shown less fluctuation in the number of average vulnerabilities, but overall, it is steadily growing. Only in November 2024, when there was a spike in the average number of vulnerabilities across the board, did this segment dip below the average. Within a segment where remediation and patching must have strict change control, testing and scheduling constraints don't make it easy to reduce the overall vulnerability count.



Average Critical Vulnerabilities per Asset for Healthcare

The average number of vulnerabilities per asset shows the constant need for vulnerability management. Still, the average Critical vulnerability count per asset highlights the immediate risk exposure across healthcare. Our data leverages real-time threat intelligence for the vulnerability findings and helps to elevate the most exploitable and riskiest vulnerabilities as Critical. These are ones where Intruders can easily gain control of the host, which can lead to a compromise in network security. For example, vulnerabilities at this

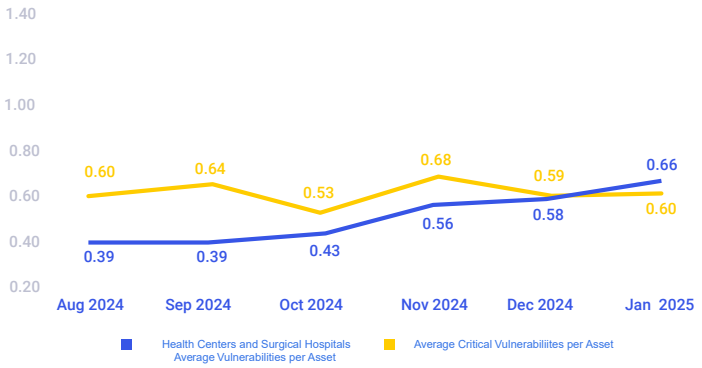
level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

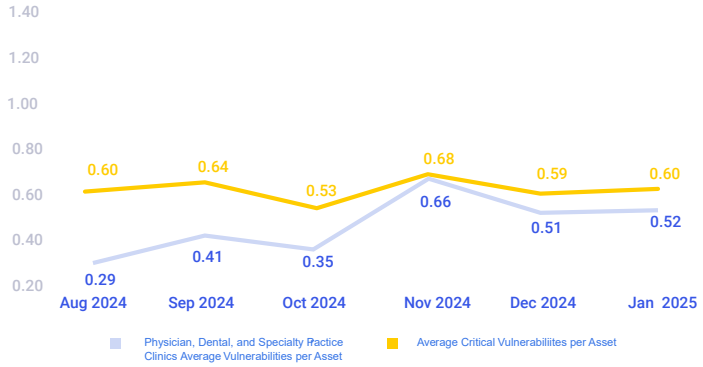
From the average over the last 6 months, **almost 3 out of every 5 assets have a Critical vulnerability finding**.

Average Critical Vulnerabilities per Asset by Segment

Healthcare Centers and Surgical Hospitals

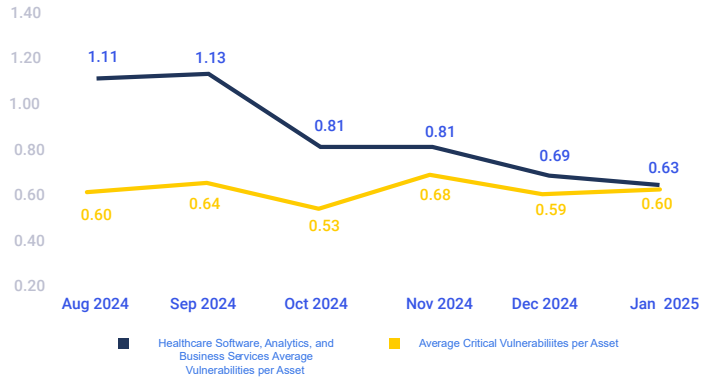
For Healthcare Centers and Surgical Hospitals, the breakdown of the Critical vulnerability findings tells a very different story compared to the vulnerability total averages in this segment. Total vulnerability averages in this segment were mainly above the average trend line for all organizations. Here, when looking at Critical vulnerabilities, this segment does much better early on but seems to be losing ground and is increasing in the carry-over of these vulnerabilities' month to month. We know this is the most constrained segment for vulnerability management and remediation activities due to the larger quantities of assets and the need for strategic change management and scheduling to minimize any service disruption potential.





Physician, Dental, and Specialty Practice Clinics

In comparison to other segments detailed in this report, Physician, Dental, and Speciality Practice Clinics are much better at managing and remediating the Critical vulnerabilities in their environments. They are consistently below the trend average. There was a peak in November, which all segments experienced, but this segment was able to remediate these Critical vulnerabilities in the following months quickly. However, they could not bring this down to the August level.

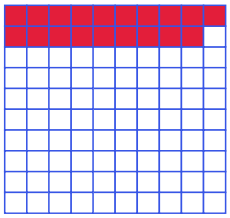


Healthcare Software, Analytics, and Business Services

Healthcare Software, Analytics, and Business Services are moving much quicker than the other segments when it comes to improving their critical vulnerabilities per asset. This segment made steady improvement, reaching just above the trend average in January 2025.

Top Performers by Segment for Managing Critical Vulnerabilities

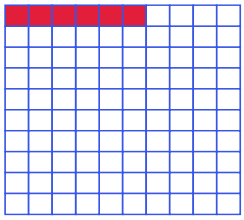
Clearwater's data shows the challenges and unique data points across the healthcare segments and how they differ in vulnerability management. However, we also wanted to share within each segment not only the average but how the top performers in each are performing. This data takes the top 10% of the best performing organizations based on managing Critical vulnerabilities and shows how they relate to the others in their respective segment. The data reflects the Critical vulnerabilities during January 2025.



Healthcare Centers and Surgical Hospitals

The top 10% experienced 19 out of 100 assets with Critical vulnerabilities.

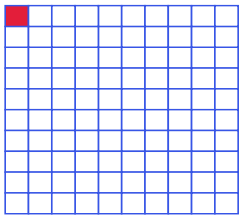
The average for Healthcare Centers and Surgical Hospitals saw 66 out of 100 assets with Critical vulnerabilities.



Physician, Dental, and Specialty Practice Clinics

The top 10% experienced 6 out of 100 assets with Critical vulnerabilities.

The average for Physician, Dental and Specialty Practice Clinics saw 52 out of 100 assets with Critical vulnerabilities.



Healthcare Software, Analytics, and Business Services

The top 10% experienced 1 out of 100 assets with Critical vulnerabilities.

The average for Healthcare Software, Analytics, and Business Services saw 63 out of 100 assets with Critical vulnerabilities.

Recommendations

Not every organization has the resources to achieve the level of vulnerability management we observed, where only one Critical vulnerability exists for every 100 assets. But there are steps you can take to make improvements in how you are managing vulnerabilities.

Here are a few ways to leverage the data in this report to inform the goals of your vulnerability management program:

Perform Vulnerability Scanning Often

New vulnerabilities are growing rapidly. Monitor your exposure risk with at least monthly scanning and, for critical systems, daily or hourly. Having fewer vulnerabilities per asset is what is desired. However, this shouldn't be because your vulnerability scanning is overdue. Also, network-based scanning doesn't provide as much detail as agent-based scanning. When possible, we recommend agent-based scanning because of the higher fidelity and the delivery of a more complete picture for managing vulnerability risk.

Prioritize the Remediation of Critical Vulnerabilities Based on Organizational Risk

Every organization is unique. The same vulnerability on a similar system could represent a very different exposure risk, even within the same healthcare segment and similar organizations. A risk-based approach must look at the function the vulnerable asset performs for the business, what type of data or processes could be exposed, and whether constraints prevent immediate remediation or if there are compensating security controls that can be leveraged to mitigate the vulnerability risk. This is one of the reasons why Healthcare Centers and Surgical Hospitals have a higher average critical vulnerability rate than the other segments. Some vulnerabilities cannot be patched immediately, and a vendor may need to upgrade a system to remediate the vulnerability. It is important to have a way within your organization to review these deferred vulnerabilities and a process to re-evaluate the vulnerabilities at a consistent time interval to ensure the risk is still acceptable or confirm that the compensating remediation is still working.

Elevate your Vulnerability Management Program

As you have seen with our findings, vulnerability management has its ups and downs. Have a plan to address what your organization might need if there were a larger-than-normal volume of risk-prioritized vulnerabilities to address, akin to storm preparedness. A monthly running count of the remediated vulnerabilities is insufficient for modern vulnerability management because of unforeseeable fluctuations. Set a threshold, review how your organization performs to the segment data in this report and look at your carryover vulnerability risk on a month-to-month basis and plan appropriately.