Cobalt

State of Pentesting in Healthcare 2025

Executive Summary

The healthcare industry is better than most industries at preventing serious vulnerabilities, but lags behind in quickly resolving findings from penetration tests, leaving organizations at risk for longer periods of time.

To help understand the security posture of the healthcare industry, we analyzed the results of thousands of Cobalt pentests over the past 10 years, and supplemented pentest data with surveys of security leaders and practitioners.

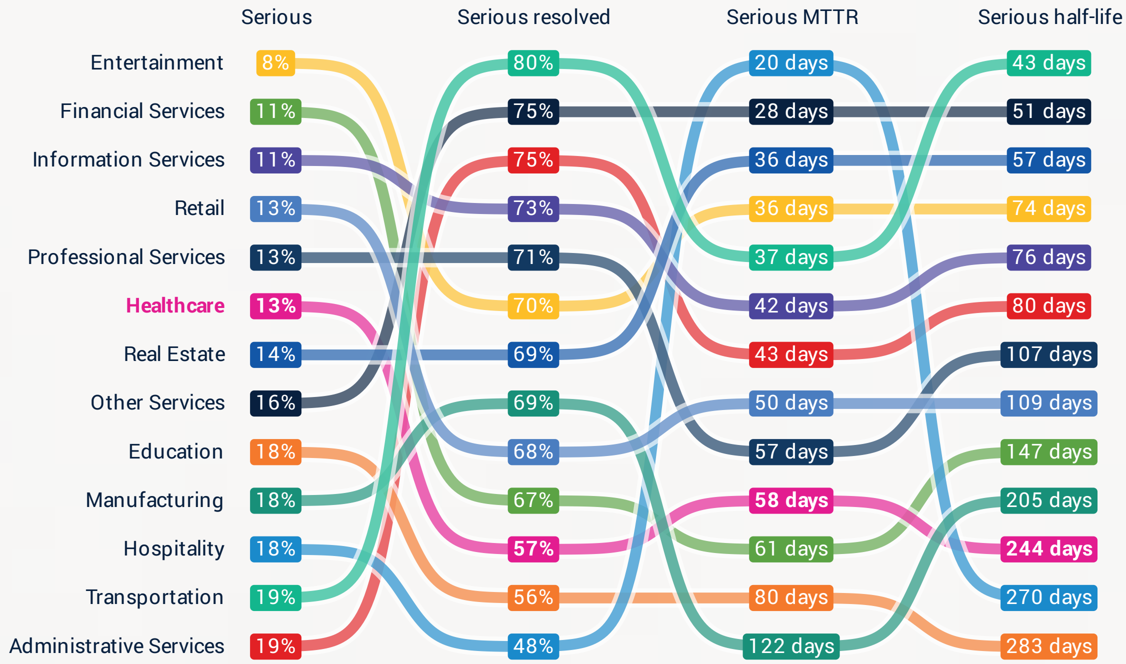
- Pentest results across 13 industries suggest that, while healthcare organizations are ahead of the curve on the rate of serious pentest findings (sixth-best out of 13 industries), security teams in this sector struggle to remediate findings quickly (11 out of 13 industries). This slow pace of remediation could be due to a range of factors, such as organizational limitations, tech debt, or resource constraints.
- Most healthcare organizations meet remediation deadlines specified by their service level agreements (SLAs). But when delays occur, they may introduce organizational risks to compliance and security.

Pentest Findings in Healthcare: Vulnerability Rates, Fix Rates, and Resolution Time

Our alluvial diagram "subway plot" graphic (Figure 1) summarizes how healthcare organizations stack up against 12 other industries. Follow the colored subway lines from left to right to read the data for each industry—healthcare is in pink–in four key metrics. The chart shows:

- Frequency of highest-risk (serious) vulnerabilities among pentest findings
- Resolution rate for serious pentest findings
- Median time to resolve (MTTR) serious findings
- Half-life (time to resolve 50% of serious findings)

Industry Comparison of Key Pentest Remediation Metrics



Source: State of Pentesting Report 2025

As **Figure 1** shows, healthcare organizations perform on par with other industries when it comes to detecting vulnerabilities classified as serious, but underperform other industries in fixing these vulnerabilities and implementing fixes quickly, resulting in a long MTTR and half-life for resolving issues.

[1] State of Pentesting Report 2025, Cobalt, April 2025.

[2] Survey of 500 security leaders and practitioners, conducted in early 2025 by Emerald Research Group, on behalf of Cobalt.

Healthcare Has a Lower Rate of Serious Findings

Cobalt pentest data shows that 13.3% of healthcare findings qualify as “serious,” the highest risk. In this metric, a lower rate is better, and healthcare’s rate of serious findings is sixth-lowest among the 13 industries we analyzed.

Serious findings rate: 13.3%
Rank: 6 out 13

Healthcare Lags on Resolution of Serious Findings

While healthcare pentests uncover fewer serious findings than most sectors, the industry lags behind many in resolution rates. A higher rate of resolving findings is better, yet healthcare organizations have the eleventh-highest rate for all industries surveyed, at just 57.4%. This falls significantly short of the top-performing industries, led by transportation (80.2%). The combination of low findings with low resolution of findings places healthcare in the “Struggling” quadrant, as seen in Figure 3.

Resolution rate: 57.4%
Rank: 11 of 13

Industry Comparison: Frequency vs. Resolution Rate of Serious Findings

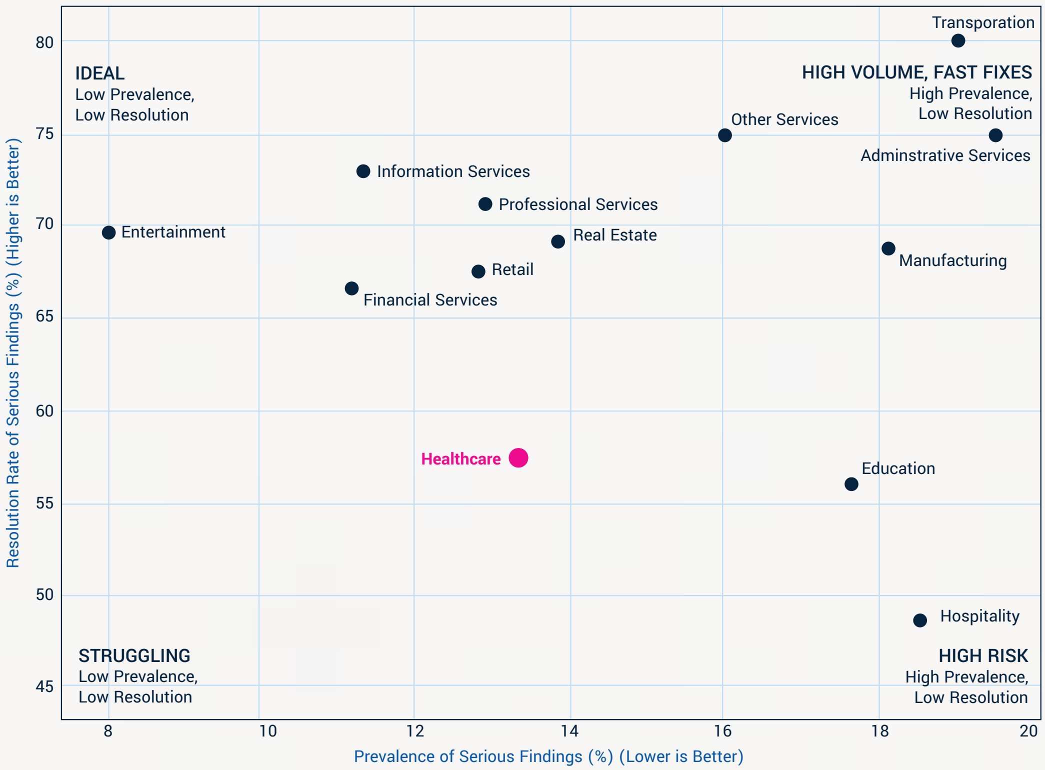


Figure 2. The scatterplot chart of industries shows where they fall on two axes--prevalence of serious findings and resolution of serious findings. Based on these plots, industries are categorized in four quadrants: “Ideal” (low prevalence of findings, high resolution of findings), “High Volume, Fast Fixes” (high prevalence, high resolution), “High Risk” (high prevalence, low resolution), and “Struggling” (low prevalence, low resolution). Source: Cobalt pentests.

Healthcare Is Slow to Resolve Serious Findings

Healthcare's organizations' low resolution rate is compounded by longer times to resolve findings they actually fix. Healthcare's MTTR for serious findings is 58 days. A lower ranking is better, but healthcare ranks fourth-highest MTTR among 13 industries surveyed, ahead of only financial services (61 days), education (80 days), and manufacturing (122 days). In contrast, the top-performing industry, hospitality, has a median resolution time of 20 days.

Median Time to Resolve Serious Findings By Industry

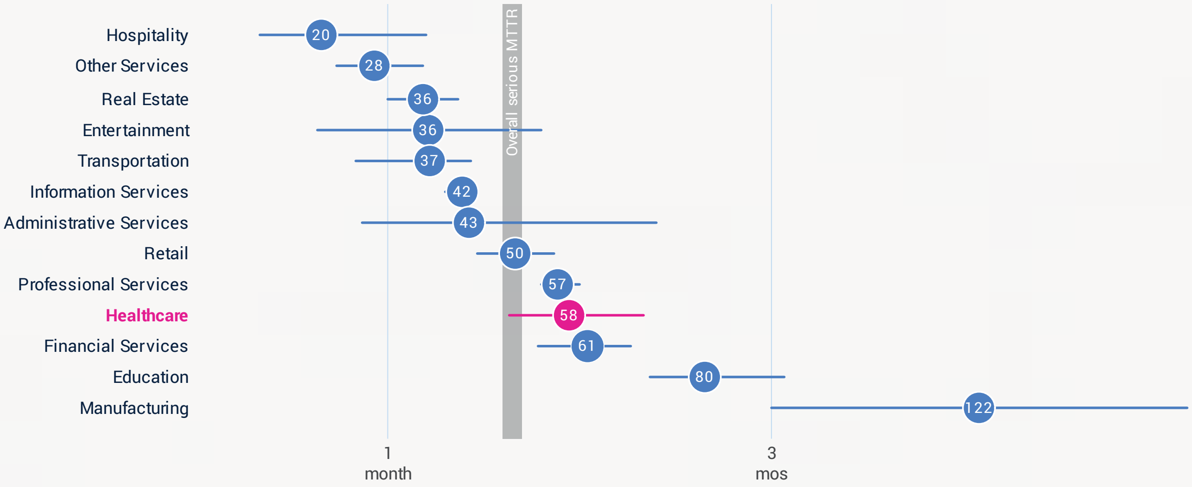


Figure 3. The dots represent MTTR, while the lines extending from each dot represent 95% degree of confidence due to sample sizes. Source: State of Pentesting Report 2025

Healthcare Accumulates Security Debt of Unresolved Serious Findings

Healthcare organizations' slowness to resolve serious findings translates into a backlog of unresolved issues, reflected in a long half-life of serious findings. Unlike MTTR, which is a measurement of the median time to resolve issues that have already been fixed, half-life is a metric measuring the time it takes to resolve 50% of all serious findings (including those still unresolved). In this way, half-life shows a more complete picture than MTTR of how well an organization is resolving the vulnerabilities it finds MTTR only measures the time to resolve issues an organization has already fixed, leaving out issues that are as yet unaddressed.

Healthcare serious findings have a half-life of 244 days, ranking 11 out of 13 industries surveyed, ahead of only hospitality (270 days) and education (283 days). In contrast, the top-performing industry, transportation, resolves half of serious findings in an average 43 days.

Half-Life of Serious Findings By Industry (Days)

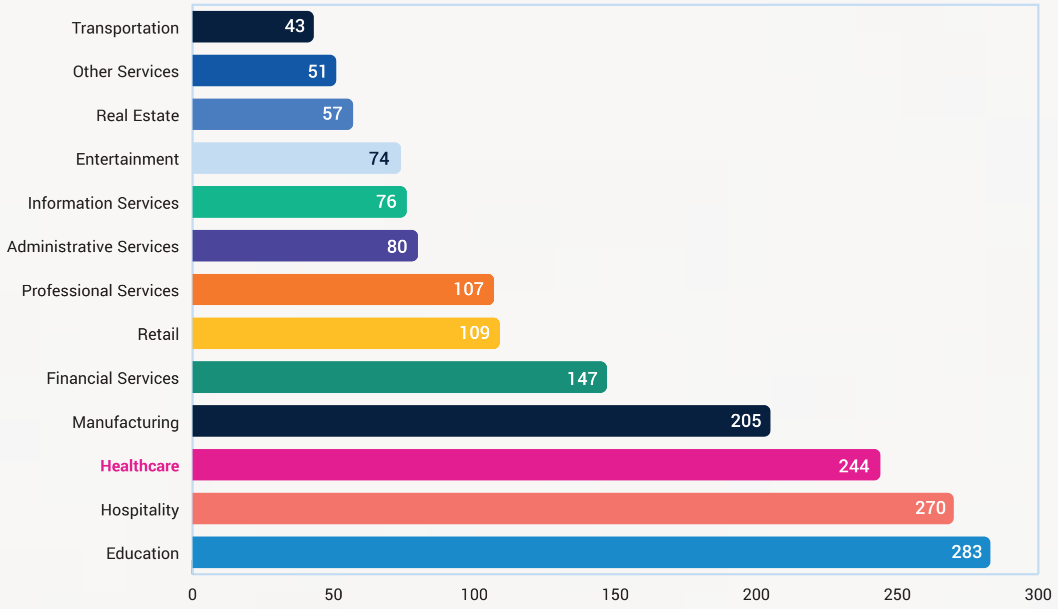


Figure 4. Source: State of Pentesting Report 2025

Survey Says: Healthcare Risks and Pentesting Practices

Top Concerns of Healthcare Leaders and Practitioners

IT risks	Attack vectors	GenAI risks
1. GenAI (71%)	1.Third-party software (68%)	1. Data exposure (46%)
2. Third-party software (48%)	2. AI-enabled features (45%)	2. Model poisoning (43%)
3. Exploited vulnerabilities (40%)	3. Phishing and malware (32%)	3. Training data leakage (37%)
4. Insider threats (39%)	4. Migration to cloud (29%)	4. Bias in AI (30%)
5. Nation state actors (27%)	5. IoT devices and embedded systems (26%)	5. Inaccurate data (29%)

Figure 5. Source: Survey of security leaders and practitioners

Healthcare Usually Meets SLA Deadlines for Business Critical Assets

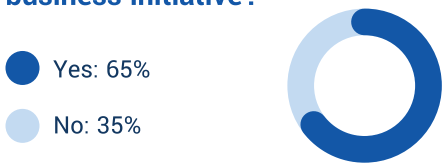
Despite slow resolution times, healthcare organizations usually manage to meet deadlines dictated by SLAs. Most healthcare SLAs require organizations to fix serious findings of business-critical assets in three days or less (39% of organizations) or four to 14 days (40%). On average, most healthcare organizations fix serious findings in business-critical assets in one to three days (43%), four to seven days (37%), or eight to 14 days (14%).

94% of healthcare organizations fix serious findings in business-critical assets in two weeks or less.

Pentest Scheduling Delays Cause Security and Compliance Difficulties

Many organizations say that scheduling pentests has rarely been an issue (35%). However, nearly two-thirds (65%) say that pentest scheduling has occasionally or frequently delayed security, compliance, or business initiatives.

Has pentest scheduling delayed a security, compliance, or business initiative?



Why Does Healthcare Find Fewer Serious Issues But Resolve Them More Slowly?

Regulatory pressure may help explain the low prevalence of serious findings in the healthcare industry. Rules such as the Health Insurance Portability and Accountability Act (HIPAA) have forced healthcare organizations to protect patient data by proactively assessing risk and preventing vulnerabilities.

A wider variety of issues may be at play in the industry's low resolution rates and slowness to resolve issues. Relevant factors include:

- Divisions between departments ordering pentests and teams implementing fixes
- Difficulties less mature teams face at managing the complexity of remediations
- Technology roadblocks from legacy systems
- Resource constraints

Fortunately, healthcare organizations can mitigate these issues by tapping into external resources provided by pentesting services. The Cobalt pentesting as a service (PTaaS) platform enables healthcare organizations to leverage our elite pentester community and schedule pentests in as little as 24 hours.

Recommendations for Security Leaders

Based on the findings in the State of Pentesting in Healthcare 2025, healthcare security leaders should adopt a more proactive, offensive security posture to address key weaknesses in vulnerability remediation and safeguard against emerging AI threats.

1

Mandate and scrutinize third-party pentesting
Given that 68% of healthcare organizations are concerned about third-party software as an attack vector, require vendors to provide comprehensive pentesting reports before procurement and throughout the software development lifecycle.

2

Integrate pentesting into the development lifecycle
To counteract slow remediation times, embed security into your development process (DevSecOps). Use targeted pentests for new features and secure code reviews for all software in development to identify and fix vulnerabilities before they reach production environments.

3

Proactively test for AI and genAI vulnerabilities
With 71% of healthcare leaders viewing genAI as a top IT risk, it's essential to proactively test new AI applications and LLMs to prevent sensitive data exposure and other vulnerabilities.

4

Adopt a programmatic approach to offensive security
Move beyond ad-hoc testing to a structured program that provides continuous visibility into your risk posture. This is crucial for an industry that struggles with a long half-life for resolving serious findings (244 days). Regular, programmatic testing can help manage and reduce security debt.

5

Conduct red team exercises
To test your organization's real-world detection and response capabilities, conduct red team exercises that simulate advanced attack scenarios.

About Cobalt

Cobalt is the pioneer in pentesting as a service (PTaaS) and a leader in offensive security services.

We are focused on combining talent and technology with speed, scalability, and expertise. Thousands of customers and hundreds of partners rely on the Cobalt Offensive Security Platform, along with the industry's largest exclusive community of 450+ trusted pentesters and security experts, to find and fix vulnerabilities across their environments. By enabling faster pentest launches, real-time collaboration with testers, continuous scanning, and seamless integration with remediation workflows, we help organizations identify critical issues and accelerate risk mitigation so they can operate fearlessly and innovate securely.

State of Pentesting Report 2025

The seventh annual State of Pentesting Report offers insights into how businesses use pentesting—and what pentesting reveals about the state of their security programs.

DOWNLOAD THE REPORT