DNSFilter



THE VISIBILITY DEFICIT SURVEY SERIES

Seeing the Risk, Missing the Signal: AI Security in Healthcare

Healthcare security teams know where their AI risk is, but they're missing the visibility into when the risk actually manifests.

The Risk Is Known

83%
use three or more AI tools for work

53%
worry about losing IP through AI training data, vs. 31% in other industries

50%
name AI security and governance as a top security gap

AI is part of everyday healthcare work. Among the surveyed IT and cybersecurity leaders in healthcare organizations, **every organization uses at least one AI tool, while 83% use three or more and 30% use between six and ten.**

Healthcare also knows where that creates exposure. **53% of respondents name the loss of intellectual property through AI training data as a top AI risk**, compared with 31% in other sectors. No other question in the survey shows a wider gap between healthcare and all other industries. Looking ahead, 43% say employees sharing sensitive data with public AI models is the biggest emerging risk of the next 12 months.

Half name AI security and governance one of their biggest security gaps, the highest share of any large sector we surveyed. The awareness is there. Visibility is the problem.



The Signal Is Missing

23%
catch SaaS and AI incidents through employee reporting, vs. 44% in other industries

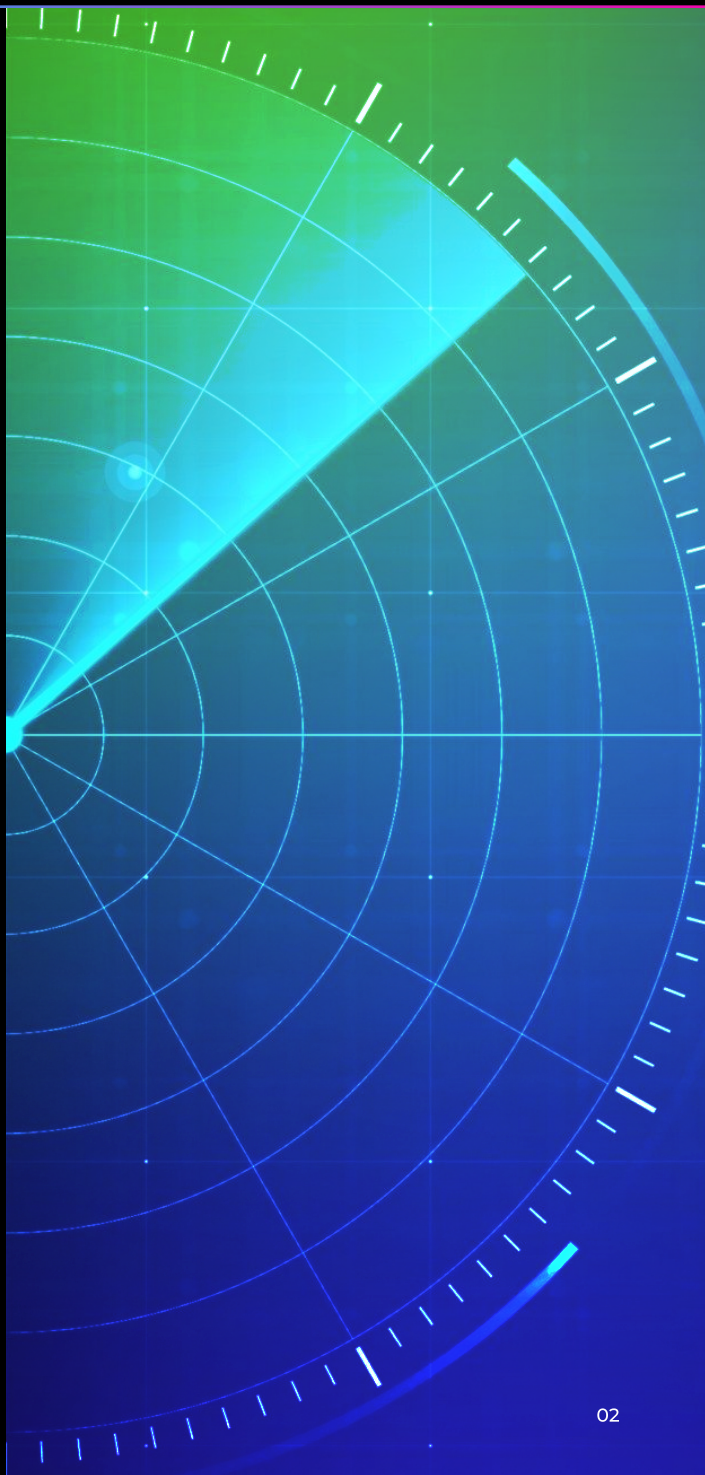
40%
say half or fewer of their security tools are actively monitored, vs. 23% in other industries

50%
have confirmed or suspect an unapproved AI tool connection

Healthcare hears about problems from the outside. **Only 23% of healthcare organizations use employee reporting to identify incidents involving SaaS or AI tools,** compared with 44% in other industries. Instead, 60% rely on vendor security notifications, as opposed to 43% in other sectors.

The tools already in place don't make up the difference. Only 27% of healthcare respondents can say every security tool they own is actively monitored, and **40% say half or fewer are, compared with 23% in other industries.** A tool nobody is watching **can't raise an alert**.

Shadow AI fills the gap. 27% have confirmed that an employee connected an unapproved AI tool to critical systems such as Google Workspace, Microsoft 365, or SSO. Another 23% suspect it but can't confirm it, which suggests many teams lack the visibility to be sure. Policy isn't stopping it either: 70% have a formal AI policy, but only 40% enforce it consistently, the lowest rate of any large sector. And in 47% of healthcare organizations, employees can grant a new AI tool OAuth or API access on their own. You can't enforce a policy against connections you can't see, which is especially concerning in an industry where the critical data needing protecting is protected health information (PHI).



Confidence Without Coverage

87%
are confident they would detect a breach within six hours

33%
had an incident originate from a SaaS or AI tool in the past 12 months

33%
have had an incident that was never formally reported or disclosed

Despite those gaps, healthcare security leaders trust their defenses. **87% are confident they could detect a breach within six hours,** and 40% call themselves very confident.

The incident record is less reassuring. One in three healthcare organizations had a security incident originate from a third-party SaaS or AI tool in the past year. The same share have had an incident that was never formally disclosed, and another third have downplayed an incident because they lacked the resources to fix it. 10% say an unapproved AI connection has already caused an incident. This gap between confidence and incidents shows up across the industries we surveyed, but in healthcare it sits on top of thinner internal visibility.

Healthcare is also less worried than its peers about several AI-driven threats. Only 13% name AI-enabled phishing as a top emerging risk, compared with 35% in other industries, and **33% are concerned about AI costs that procurement and security monitoring can't see,** compared with 56% elsewhere. Lower concern doesn't mean lower risk; it may simply mean the risk is harder to see.



You Can't Protect What You Can't See

Healthcare already knows AI governance is its biggest gap. Before the next dollar goes toward closing it, three questions are worth answering:

- Which AI services are your users reaching today, and what data is going to them?
- Would you hear about a problem from your own team, or from a vendor?
- Is your AI policy enforced, or only written down?

DNS-first security gives healthcare security teams answers to all three.

See every AI service on your network.

START A FREE TRIAL OF LUMINATE BY DNSFILTER™.



The Money Isn't Following

33%

are sending their next dollar to AI security and governance, vs. 41% in other industries

7%

grew their security budget by more than 10%, vs. 20% in other industries that grew their budgets by the same margin

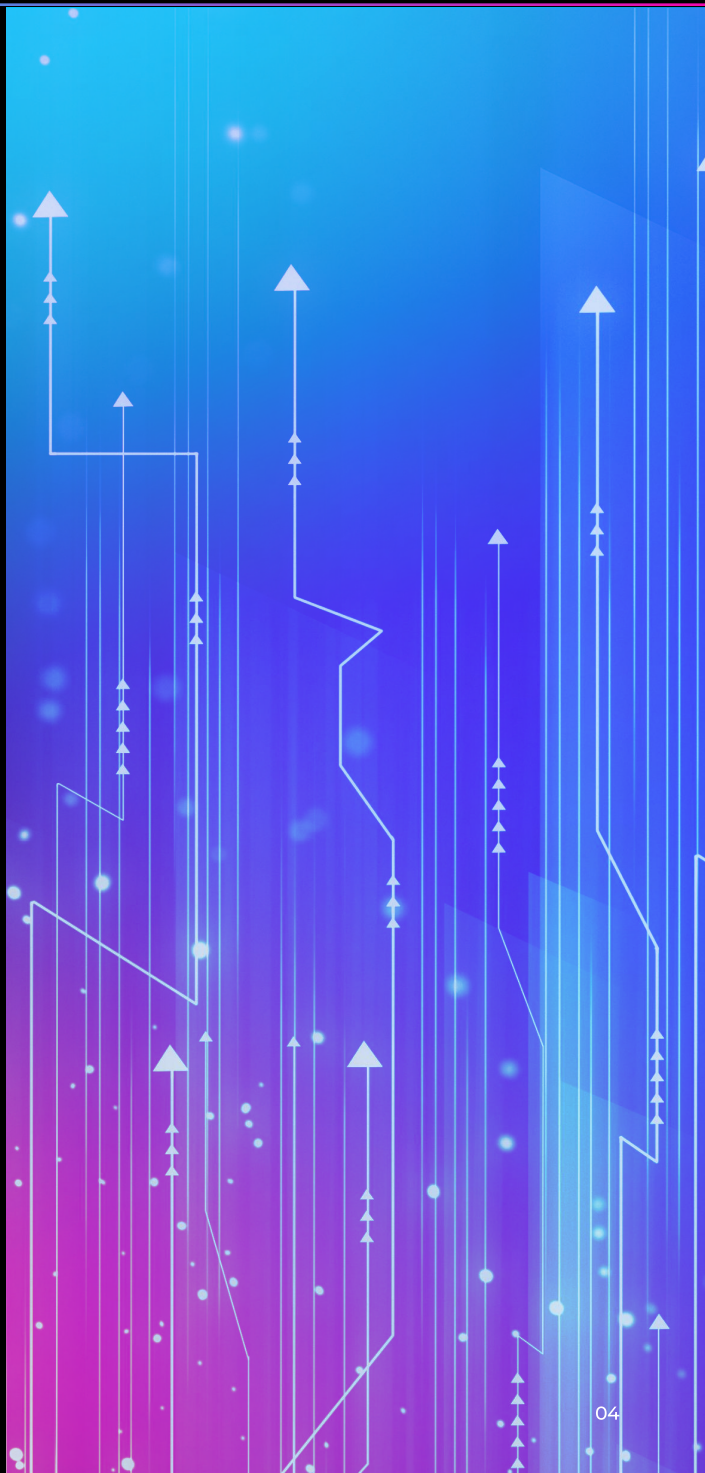
57%

could not maintain critical operations through a 72-hour disruption

Healthcare names AI governance as its biggest gap more often than any other large sector, but it's putting less new money there. **Only 33% of healthcare organizations say their next security dollar goes mainly to AI security and governance,** compared with 41% in other industries.

Part of the reason may be the size of the budget itself. 70% of healthcare organizations increased their security budget over the past year, but most increases were modest. **Only 7% grew spending by more than 10%, compared with 20% of other industries that significantly increased theirs.** Meanwhile, 10% of healthcare organizations saw their security budget shrink, compared with 2% elsewhere.

The stakes make this gap harder to ignore. If a major cyber attack disrupted core operations for 72 hours or more, **40% of healthcare organizations say they would keep critical operations running, and 17% expect critical failures within 24 hours.** In most industries, an outage disrupts business. In healthcare, it can delay patient care.



Methodology



Survey data

In June 2026, DNSFilter partnered with Censuswide to survey 400 IT and cybersecurity professionals across the US and Canada. Respondents held manager-level roles and above at companies with 150 to 5,000 employees, across all industries. This report focuses on the 30 healthcare respondents and compares their answers with those of the 370 respondents from 12 other industries. Percentages are rounded to the nearest whole number.

Get in touch

dnsfilter.com/contact
(877) 331-3412
sales@dnsfilter.com