SECTION 04

AI attacks are mainstream. AI defenses are not.

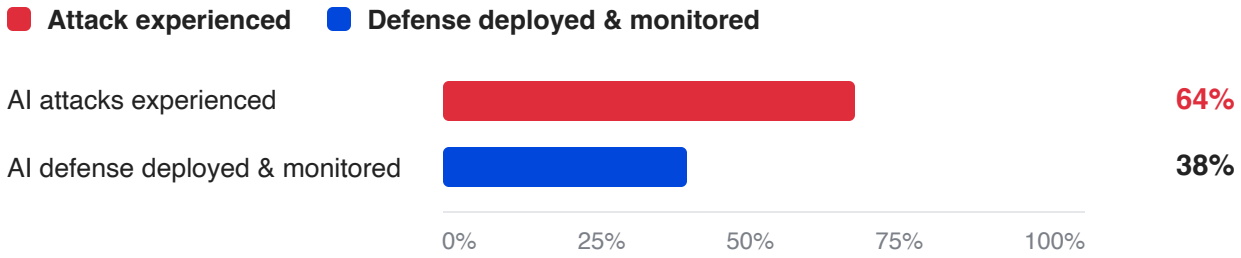
64% of healthcare organizations have experienced an AI-generated or AI-enhanced email attack. Only 38% have AI-based defenses fully deployed and monitored.

A 26-point gap between attack and defense

AI attack prevalence is outpacing AI defense operationalization.

AI email attack vs. AI email defense

Experienced attack vs. fully deployed and actively monitored defense (n=170).



Nearly 4 in 10 respondents confirmed an AI-driven attack. 1 in 4 suspected but could not confirm. 28% said no, and 8% were unsure.

On the defense side, 38% have AI or machine learning for email threat detection fully deployed and actively monitored. Another 37% have AI defenses deployed but not monitored or tuned. The remaining quarter are evaluating, not adopting, or unsure.[4]

The asymmetry is an operational maturity gap. Unmonitored AI detection is not the same as AI detection tuned against real email traffic. By the tuning standard, roughly 6 in 10 organizations are running behind the threat.

44% → 75%

AI adoption has climbed fast. In Paubox's June 2025 "Dangerously Overconfident" report, 44% had deployed AI/ML for threat detection.[6] Nine months later, 75% have some form of AI defense. Only 38% have it fully monitored.

▲ +31pts

The attacker side is not waiting

The FBI's warning describes exactly what healthcare IT leaders are already seeing. IBM's numbers describe the cost.

> "AI technology enables the creation of convincing synthetic content, such as social media profiles and personalized conversations, often in mass quantities."
>
> **FBI Internet Crime Complaint Center (IC3)**
> December 2024 Public Service Announcement[2]

$7.42M

Average healthcare data breach cost in 2025. The highest of any sector for the 14th consecutive year. Phishing is the leading initial access vector.[3]

64%

Of healthcare organizations report AI-generated or AI-enhanced email attacks. The "mass quantities" the FBI warned about are already landing in healthcare inboxes.[4]

Closing the AI detection gap is an investment against a cost healthcare already pays. Every month the gap stays open is another month of AI-generated phishing landing in inboxes that are defended by rules written for an earlier class of threats.

The 1 in 4 organizations that have AI defense deployed but not monitored are technically checking the box without meaningfully reducing risk. Operationalization is where the actual defense happens.

PAUBOX

Secure every email you send and receive

Paubox combines healthcare compliance with AI to protect organizations from the most sophisticated attacks.

Talk to an expert