Average cost of a data breach in the **healthcare industry**

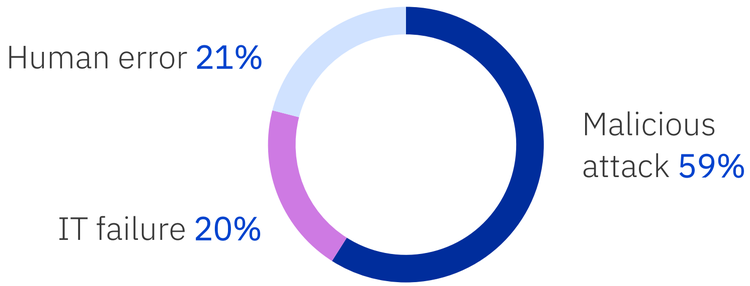
USD 6.64M

Highest cost of 17 industries studied

25% higher than the USD 4.99M global average

11% lower compared to 2025

Root causes of a data breach



Time to identify and contain; healthcare industry

Global findings

Key statistics

56%

Increase in breaches involving AI-generated attacks

85%

Share of breached organizations that plan to increase security spending in response to potential threats from frontier AI models

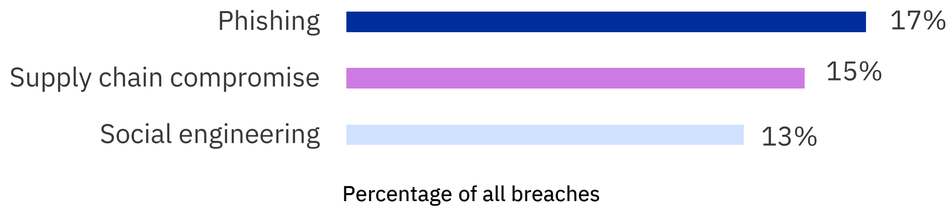
36%

Percentage of global organizations with extensive use of security AI and automation

USD 1.93M

Global cost savings of extensive use of security AI and automation versus no security AI and automation

Top three initial attack vectors



Time to identify and contain; global average

Recommendations

- **Operate security at the speed of AI-driven attacks by embedding AI across the entire security lifecycle**, including vulnerability management, detection and response. As exploitation timelines shrink from months to minutes, organizations must reduce decision latency and automate containment to minimize breach impact.
- **Apply agentic AI to proactively identify and remediate vulnerabilities across systems and software pipelines**, prioritizing high-risk exposures before they are exploited. Integrating AI into vulnerability management enables continuous, autonomous defense and reduces reliance on reactive security models.
- **Shift identity and access management to continuous, risk-based runtime verification**, replacing static controls with real-time access decisions. Secure both human and non-human identities (NHIs), including AI agents, through just-in-time access, anomaly detection and lifecycle governance.
- **Establish robust governance for AI agents through structured discovery, onboarding and monitoring**, ensuring visibility into how agents access systems and data. Implement authentication delegation, authorization policies and continuous activity tracking to reduce misuse risks.
- **Adopt AI sovereignty principles to maintain control over data, models and execution environments**, ensuring consistent security policies across hybrid and multicloud infrastructures. Clear visibility into where AI operates and how data flows is critical to reducing systemic risk.
- **Strengthen application and API security to support AI-enabled ecosystems**, enforcing trusted identity across users, services and AI agents while ensuring cloud workloads are securely configured and continuously monitored.
- **Implement end-to-end visibility and monitoring of data flows across AI systems**, tracking how data is ingested, transformed and exposed. This practice supports early detection of sensitive data risks and strengthens governance, compliance and secure AI adoption.
- **Prepare for post-quantum security risks by modernizing cryptographic strategies and building crypto-agility**, including discovering and securing cryptographic assets, improving key management and planning the transition to quantum-resistant encryption across environments.

Download full report →