



Secure Patient Care and Critical Health Data

The only AI SOC platform for machine-speed defense

Healthcare organizations operate some of the highest-stakes security environments — the systems they defend keep patients alive — and attacks against them now move faster than any human team can answer. At the same time, the rules protecting patient data keep tightening, and every action a security tool takes has to be documented and defensible, the kind of evidence an OCR audit or a breach investigation will demand.

That's the gap healthcare security leaders have to close: machine-speed attacks on one side, human-speed response and manual compliance on the other. This paper lays out why healthcare is uniquely exposed, what separates a real AI SOC from the tools claiming the label, and how the Torq AI SOC Platform closes the gap in production today.

Why Healthcare Is a High-Risk Target

No industry pays more when it's breached. The average healthcare data breach reached \$7.42 million in 2025, the highest of any sector and a dubious distinction healthcare has held for 14 straight years.¹ And the threat is accelerating on every front:

The Change Healthcare ransomware attack, the largest in healthcare history, ultimately affected 192.7 million people — nearly two-thirds of the U.S. population.²

772 large healthcare data breaches were reported in 2025 alone.³

Confirmed U.S. healthcare ransomware incidents reached 460 in 2025.⁴

74% of IT professionals say hiring cybersecurity staff is a significant workforce challenge.⁵

What sets healthcare apart is what sits downstream of the breach. When ransomware locks an EHR or takes a claims system offline, the damage isn't measured only in records exposed; it's measured in delayed procedures, rerouted emergencies, and care that can't be delivered.

Slow response compounds all of it. Across industries in 2025, organizations took an average of 241 days to identify and contain a breach, and those that ran past the 200-day mark cost \$5.01 million on average, versus \$3.87 million for those caught sooner.¹ In healthcare, not only does the lag cost money, it puts patients at risk.

Healthcare SOC's can't hire their way out of this. Alerts pile up faster than analysts can clear them, and every minute in the queue is a minute an attack moves closer to the systems patients depend on. It's why 85% of security leaders now want a single AI SOC platform they can trust to keep pace.⁶

WHAT AN AI SOC ISN'T — AND IS

Most tools marketed as an “AI SOC” stop at triage. They prioritize alerts, generate a recommendation, and hand the real work back to a human. The investigation still happens by hand, the response still means logging into another tool, and the case still closes on human time. The bottleneck moves; it doesn't disappear. Others simply bolt a chatbot onto legacy architecture or hide their reasoning inside a black box — a non-starter in an industry where every decision has to be explained to an OCR auditor.

A true AI SOC carries the alert through to the end. It investigates, correlates evidence, takes containment and remediation actions across the stack, and escalates to a person only when human judgment is genuinely required, with every step grounded in context, logged, and reversible. The test is simple: if it can't take action, it isn't an AI SOC. In healthcare, that distinction is the whole point, because the value of autonomy is closing the window between when an attack starts and when it's stopped, before it reaches the systems that keep patients safe.

The Torq AI SOC Platform for Healthcare

The Torq AI SOC Platform runs the entire threat lifecycle — triage, investigation, response, and remediation — with agentic AI operating under your team's direction. It integrates with the stack you already own, produces the audit-ready evidence HIPAA demands, and is built for the distributed environments healthcare actually runs in.

Built-In Compliance and Auditability

Healthcare operates under a dense, overlapping set of requirements: the HIPAA Security Rule, HITECH, SOC 2, and an evolving patchwork of state and federal rules, with The Health Care Cybersecurity and Resiliency Act of 2025 raising the bar further.

Torq builds audit-ready evidence into every agentic action. Torq HyperAgents™ log their full reasoning chain — every step, every verdict, every action — and native case management preserves a full chain of custody, turning daily operations into a continuous compliance record instead of a pre-audit scramble.

Transparency and Control

Trust has to be earned before an organization will let a system act. Torq HyperAgents operate under explicit direction: you define the agent's role, permissions, escalation boundaries, and authorized actions. Analysts review the reasoning and evidence behind every action in real time, with override always available, and adjustable autonomy lets a team start conservatively and extend the platform's authority as confidence grows.

Agentic AI for healthcare's most critical use cases:

- ✓ **PHI exposure detection and response:** Detect PHI exposure signals, trigger investigations, notify the appropriate teams, and automatically quarantine affected systems.
- ✓ **Ransomware containment:** Isolate infected endpoints and lock compromised accounts before clinical operations are disrupted.
- ✓ **Secure access management:** Grant time-limited, role-based access to clinicians, remote staff, and third-party vendors, and automatically revoke it when the session ends.
- ✓ **Medical device and infrastructure threat detection:** Extend detection across a hard-to-patch medical OT fleet and launch investigations regardless of the source of the alert.
- ✓ **Compliance and audit evidence:** Automated, audit-ready evidence collection for HIPAA, HITECH, and SOC 2 by default.

Integration Without Rip-and-Replace

Torq layers on top of the complex environments that healthcare organizations already run (EHR systems, medical devices, cloud infrastructure, and remote care platforms) with more than 400 integrations across tools like Microsoft, CrowdStrike, ServiceNow, and Wiz. Where an integration doesn't exist, teams prompt Torq Socrates™ Agentic Builder in natural language to create it.

Proven in Production

Torq runs in demanding enterprise environments today, closing cases autonomously while keeping analysts in the loop for calls that require judgment. A global biopharmaceutical company operating across more than 150 countries used Torq to cut mean time to resolve by 92% and bring average alert triage to 56 seconds, while Torq's automation identified 35% of cases as duplicates and resolved them without redundant analyst effort, absorbing rising case volume without adding headcount

WHY CHOOSE TORQ?

- ✓ Agentic AI across the full threat lifecycle
- ✓ Socrates orchestrates specialized Torq HyperAgents built from natural language
- ✓ Torq Auto Triage delivers explainable verdicts that cut alert noise
- ✓ AI-native case management from investigation through case closure
- ✓ Adjustable autonomy allows for both human-on-the-loop and human-in-the-loop controls depending upon scoped preference
- ✓ Transparent, auditable reasoning with immutable logs for every verdict and action
- ✓ Audit-ready evidence built-in for HIPAA, HITECH, and SOC 2
- ✓ Enterprise-grade RBAC, approval workflows, and policy guardrails
- ✓ Grounded in the Torq Context Graph, with memory and learning that sharpen every verdict over time
- ✓ 400+ integrations with no rip-and-replace
- ✓ Coverage across EHR, medical devices and OT, cloud, and remote care
- ✓ Proven at enterprise scale, running more than one billion automated actions a week

Gartner
Peer Insights™

"The automation from data ingestion to IoC enrichment has offered us improved efficiencies on repetitive tasks, making decisions faster, and being able to utilize AI to reduce noise/ alert fatigue."

★★★★★

IT Security & Risk Management Associate
Healthcare, 3B - 10B USD

"This tool is very versatile. You can do magic with it."

★★★★★

Manager, IT Security and Risk Management
Healthcare, 30B+ USD

"The capacity of this program to detect any security challenge or anomaly is high, and this gives us the power to proactively manage ourselves."

★★★★★

Data Analyst
Healthcare, 250M - 500M USD

Secure Patient Care with Defense That Acts at Machine Speed

The Torq AI SOC Platform runs the entire threat lifecycle autonomously and audit-ready, so you protect your most valuable asset: the trust patients place in your care.

SEE IT IN ACTION

THE AI SOC CATEGORY LEADER



Leader in all four categories of the 2026 Leadership Compass: The Emerging AI SOC



The Company to Beat in AI SOC Agents for Threat Investigation, May 2026



"Torq is more or less the de facto leader of the AI SOC space."

Recognized Across the Market

PeerSpot #1-ranked AI SOC platform

Gartner Peer Insights 4.8 Stars

CRN 5-Star Partner Program

3x CRN Channel Chief

References

1 IBM, *Cost of a Data Breach Report 2025*

2 *Change Healthcare*

3 U.S. Department of Health and Human Services

4 American Hospital Association

5 SANS Research, *The Cybersecurity Talent Shortage Narrative Is Wrong. The Real Crisis Is What Your Team Doesn't Know, Starting with AI*

6 Torq, *The 2026 AI SOC Leadership Report*

About Torq

Torq is transforming cybersecurity with the Torq AI SOC Platform. Torq empowers enterprises to instantly and precisely triage, investigate, and respond to security events at scale. Torq's customer base includes major multinational enterprises such as Check Point Security, Chipotle Mexican Grill, Inditex (Zara, Bershka, and Pull & Bear), Informatica, Kyocera, Lego, Prudential, Rocket Companies, Telefónica, Uber, Valvoline, Virgin Atlantic, and Wiz.