



Defend the Trust That Powers Finance

The only AI SOC platform for machine-speed defense

Financial institutions operate some of the highest-stakes security environments on earth, and the attacks against them now move faster than any human team can answer. At the same time, the regulatory bar keeps rising, and every autonomous decision a security tool makes has to withstand scrutiny from regulators, auditors, and boards.

That's the gap financial services 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 finance 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 Financial Services Is a High-Risk Target

The cost of a breach is higher in financial services than in almost any other industry. The average financial sector data breach reached \$5.56 million in 2025, second only to healthcare and well above the global average of \$4.44 million.¹ And the threat is accelerating on every front:

Nation-state activity surged in the past year, with North Korea-linked groups tripling their attack pace and stealing more than \$2 billion in crypto assets.²

More than a third of financial-services incidents now begin with social engineering, a sign that attackers are targeting people as effectively as systems.³

Confirmed finance-sector ransomware incidents rose from 30% between 2024 to 2025, and the first quarter of 2026 was up 76% year over year.⁴

16% of breaches now involve AI-driven techniques such as automated phishing and deepfake impersonation.¹

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 finance, where a compromised wire or a frozen payment rail carries systemic weight, that lag erodes the trust the entire sector runs on.

And the lag is structural: analysts face more alerts, more tools, and more regulatory obligations than any team can work through by hand, so the response clock keeps running. That's why the traditional SOC model is buckling, and why 85% of security leaders now say they want a single unified platform they can trust.⁵

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 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 finance, 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, while producing a defensible record of every move.

The Torq AI SOC Platform for Financial Services

The Torq AI SOC Platform runs the entire threat lifecycle — triage, investigation, response, and remediation — with agentic AI under your team's direction. It integrates with the stack you already own, produces audit-ready evidence that regulators demand, and is already running in production across some of the most demanding financial environments in the world.

Built-In Compliance and Auditability

Financial services organizations operate under the strictest, most overlapping regulatory regimes of any industry: PCI DSS, SOX, GLBA, FFIEC guidance, and SEC cybersecurity disclosure rules. In addition, the EU's Digital Operational Resilience Act (DORA) has been fully applicable to financial entities since January 2025, and the EU AI Act's high-risk requirements are in effect as of August 2026.

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 institution 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.

- ✔ **Fraud and wire-transfer defense:** Detect suspicious Zelle transactions, wire anomalies, and account takeovers, then lock accounts and notify fraud teams in seconds.
- ✔ **Phishing detection and containment:** Run the full phishing lifecycle agentially, from triage and enrichment through investigation, notification, and remediation.
- ✔ **Ransomware containment:** Isolate infected systems and lock compromised accounts before an analyst opens a laptop.
- ✔ **Identity and access management:** Automate just-in-time access, stale-account cleanup, and response to suspicious identity behavior.
- ✔ **Compliance and audit evidence:** Automated, audit-ready evidence collection for PCI DSS, SOX, GLBA, and FFIEC by default.

Integration Without Rip-and-Replace

Torq layers on top of the complex environments that financial institutions already run, with more than 400 integrations across tools like CrowdStrike, Wiz, Microsoft Sentinel, SentinelOne, and ServiceNow. Where an integration doesn't exist, teams prompt Torq Socrates™ Agentic Builder in natural language to create it.

Proven in Production

After moving away from a legacy SOAR, FICO's global SOC reduced mean time to respond by 99.4% and now closes more than 75% of its cases through automation, maintaining a clean audit record.⁶ A top-30 U.S. bank launched more than 100 automations in 90 days, automating its Zelle fraud response to reinstate services after a regulatory suspension.⁷

WHY CHOOSE TORQ?

- ✓ Agentic AI across the full threat lifecycle
- ✓ Socrates orchestrates specialized Torq HyperAgents 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 PCI DSS, SOX, GLBA, and FFIEC
- ✓ 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
- ✓ Multi-tenancy, segmentation, and data-residency support for global institutions
- ✓ Proven at enterprise scale, running more than one billion automated actions a week

Gartner
Peer Insights™

"The ease of implementation, integrated cyberprotection capabilities, the customer service, and professional success team have truly impressed us."



Manager, IT Security and Risk Management
Finance 500M - 1B USD

"Torq has become the way our team ships security automation, and has performed above expectations."



VP, IT Security and Risk Management
Finance 3B - 10B USD

"It brings peace of mind knowing we have mechanisms in place that keep our organization secure because Torq is on top of everything."



Security Engineer, IT Security and Risk Management
Finance 250M - 500M USD

Secure Your Financial Institution 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 your clients place in you.

SEE IT IN ACTION

THE AI SOC CATEGORY LEADER

KuppingerCole Analysts

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

Gartner®

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

Forbes

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

Recognized Across the Market

CRN 5-Star Partner Program

3x CRN Channel Chief

PeerSpot #1-ranked AI SOC platform

Gartner Peer Insights 4.8 Stars

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 enterprise customers, including Check Point Security, Chipotle Mexican Grill, Inditex (Zara, Bershka, and Pull & Bear), Informatica, Kyocera, Lego, Procter & Gamble, Prudential, Siemens, Telefónica, Uber, Valvoline, Virgin Atlantic, and Wiz.

References

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

2 CrowdStrike, *2026 Financial Services Threat Landscape Report*

3 Palo Alto Networks, *2025 Unit 42 Global Incident Response Report: Social Engineering Edition*

4 Black Kite, *2026 Financial Services Cybersecurity Report*

5 [Torq, The 2026 AI SOC Leadership Report](#)

6 [Torq, FICO customer case study](#)

7 [Torq, top-30 U.S. bank customer case study](#)