BREACHRX

DATA SHEET

Cyber Incident Response Management

Powered by the Rex Platform™

You're prepared for attacks. You're not prepared for what happens after.

Detection is not the hard part anymore. After containment, the decisions determine your outcome, and the real exposure begins, some of which include:

- Executive and company liability
- Regulatory scrutiny and fines
- Civil and criminal litigation
- Disclosure risk in every jurisdiction

BreachRx CIRM

BreachRx Cyber Incident Response Management (CIRM) elevates incident response into a disciplined, enterprise-wide process for making consistent, repeatable decisions and making every response defensible by embedding evidence capture directly in real time. The solution provides:

- Centralized, coordinated execution across teams
- Real-time unified visibility into status, obligations, and risk exposure
- Clear ownership across security, legal, privacy, IT, communications, and leadership
- Complete, defensible documentation of decisions and actions

Without CIRM, organizations rely on meetings, chat channels, spreadsheets, and disconnected tools during their highest-risk moments

BreachRx CIRM at a Glance

- **Enterprise Incident Command Center:** Real-time authoritative command dashboard that shows clear ownership, relevant deadlines, and automated reports.
- **Cross-Functional Coordination:** Role-based workflows across security, legal, privacy, IT, and leadership to align decisions.
- **Agentic AI Decision Support:** Context-aware guidance and adaptive playbooks for faster, more consistent decisions, even with incomplete information.
- **Continuous Evidence Capture:** Automatic logging of actions, decisions, and communications for audit-ready defensibility. No reconstruction after the fact.
- **Embedded Regulatory Analysis:** Integrated disclosure logic and obligation tracking to reduce fines, missed deadlines, and overdisclosure risk.
- **Secure, Privileged Collaboration:** Segmented access and protected communication channels to preserve legal privilege.

The Incident Response Gap

Security tooling has evolved for decades — from ITSM to SIEM, EDR/XDR, SOAR, and AI SOC. Each generation improved detection, containment, and automation. But as incidents became constant, larger, and more complex, the tools remained focused on technical tasks — not enterprise decision-making.

This created the incident response gap: a disconnect between what security systems produce (alerts and tickets) and what the business actually needs — clear ownership, coordinated decisions, defensible documentation, and real-time visibility into risk. Organizations believe they have an incident command structure. In reality, they have fragmented tools built for operations, not governance. CIRM closes that gap by connecting “what security has” to “what the business needs.”

Incidents Evolved Faster than the Tools

CIRM connects “What security has” (Alerts/Tickets) to “What the business needs” (Clarity/Context)

1990s
Basic Attacks
ITSM
Built for IT Ops

2000s
Detect Attacks Better
SIEM
Built for Detection

2010s
Contain Attacks Once Detected
EDR/XDR
Built for Containment

Late 2010s
Enforce Technical Fixes
SOAR
Built for Efficiencies

2020s
Automate Tedious Tasks
AI SOC
Built for Triage

THE IR GAP

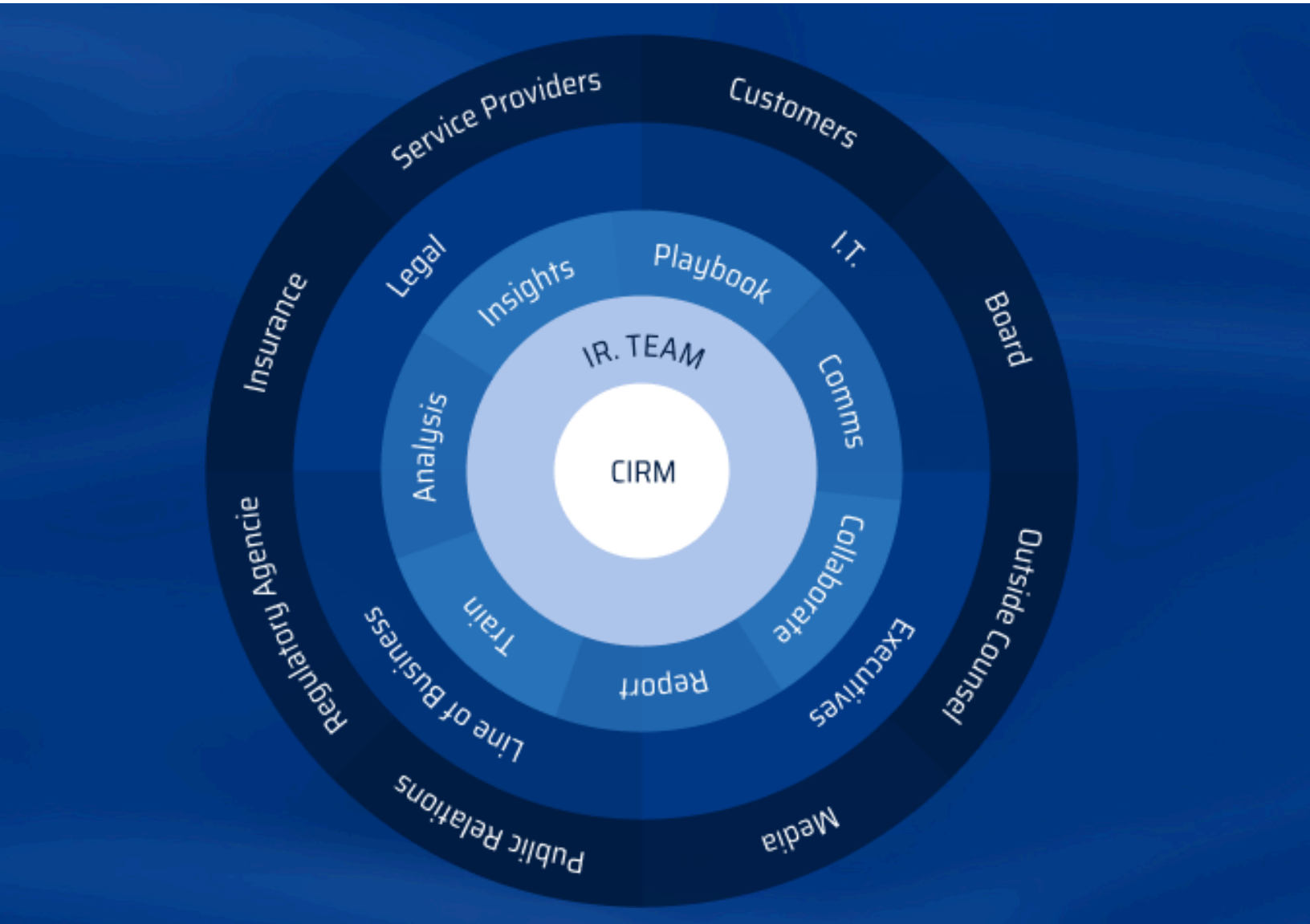
2026
Constant, Bigger Attacks
CIRM
Built to be Incident Command Center

Cyber Incidents Now Require an Enterprise-Wide Response

Cyber incidents no longer stay within security. What begins as a technical event quickly becomes an enterprise-wide event. Within hours, the legal team is evaluating contractual, disclosure, and regulatory risks. Executives want accurate updates, and communications prepare internal and public statements. But most organizations struggle to manage response at this level.

The failure is not technical execution; it is enterprise-wide coordination. As a result, decisions are made without shared context or defensible documentation. Actions live in email threads, Slack, or Teams channels, and action items and ownership are tracked manually, resulting in the fragmentation of status and accountability across disconnected tools. There is activity everywhere, but no authoritative, consolidated view. This causes a breakdown in the organization's ability to make confident, aligned decisions.

Cyber incident response is now a continuous, enterprise-wide process. Yet in most organizations, it is still managed like an ad hoc scramble instead of a consistent, repeatable discipline.



Agentic AI ensures that coordination remains disciplined — even when information is incomplete.

Agentic AI Built Into CIRM

The Rex Platform embeds agentic AI directly into the incident response lifecycle to reinforce human judgment and automate routine tasks.

The CIRM Agentic AI ensures that the response is coordinated and disciplined by:

- Continuously evaluating incident state and context, and updating tasks and deadlines
- Guiding structured, role-based workflows to enable enterprise-wide coordination
- Surfacing relevant obligations and dependencies
- so all teams are aligned on critical tasks
- Reinforcing escalation pathways to ensure the right resources are informed and involved
- Adapting playbooks as the incident evolves
- Flagging disclosure and regulatory risks in real time

Agentic AI ensures that coordination remains disciplined — even when information is incomplete.

The Rex Platform™

BreachRx CIRM is powered by the Rex Platform. The platform functions as the Enterprise Incident Command Center for cyber incidents, a system that fills the gap between what executives believe they have and what actually exists. It aligns technical responders and business stakeholders in one authoritative system and embeds defensibility directly into response execution.

CIRM Warranty

BreachRx is the only company to offer a CIRM Warranty to provide defensible incident response and financial protection when it matters most. BreachRx CIRM is purpose-built for enterprise-wide cyber response, embedding structured decision workflows, continuous evidence capture, regulatory analysis, and protected communications directly into execution. Every action is documented in real time, creating an audit-ready record that stands up to board scrutiny, regulatory review, and litigation. The result is not just faster coordination but a defensible, financially protected response designed to reduce fines, limit liability, and protect the enterprise when exposure is highest. Read more about the CIRM warranty here.

BREACHRX

AICPA SOC

SOC 2 Type II Certified

About Us

BreachRx offers the Rex Platform, an agentic AI-powered CIRM platform that orchestrates cross-functional incident response, guiding execution and ownership to enable faster containment and governance at enterprise scale.

Contact Us

info@breachrx.com

linkedin.com/company/breachrx

breachrx.com