

Closing the Loop on Incident Response with RadarFirst

In an ecosystem of security and incident management tools, RadarFirst automates incident risk assessment to provide regulatory breach notification guidance.

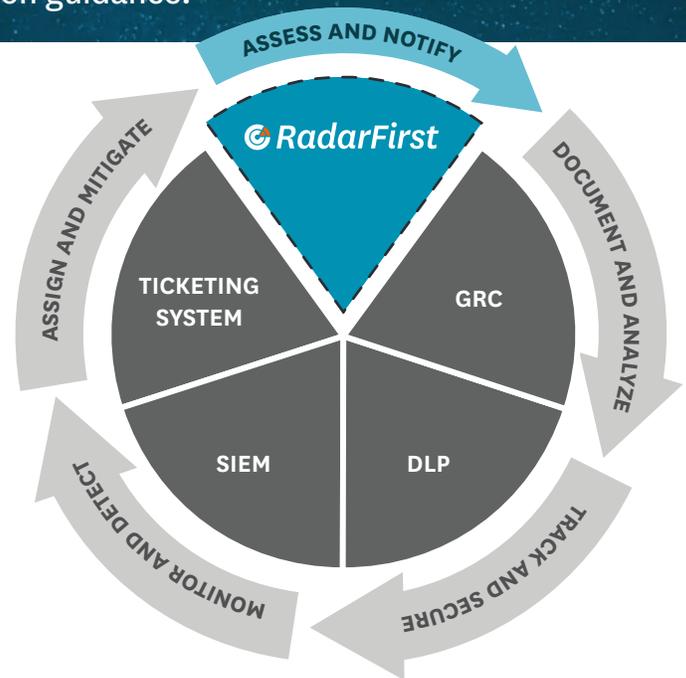
Privacy and security incidents that expose sensitive customer data have become an inevitable part of doing business in today's world.

Attacks on your company's infrastructure become more sophisticated with advancing technology – malware, ransomware, phishing schemes – while human error continues to be a leading source of incidents such as lost laptops, misdirected emails, and misplaced paper files.

Luckily, today's security solutions are rising to match this threat with an ecosystem of sophisticated products and services designed to protect and manage sensitive corporate data. A well-developed privacy and security governance program includes the use of tools such as:

- **Governance, Risk, and Compliance Platforms (GRC):** providing content management, workflow management, reporting and relational data models.
- **Security Information and Event Management Solutions (SIEM) or Managed Security Service Providers (MSSP):** providing a holistic view of IT security, with centralized storage to detect, log, analyze, and correlate security threats and trends.
- **IT Ticketing Systems:** allowing IT teams to notify multiple stakeholders in the remediation process, track and document the investigation of the event, and assign roles for remediation.
- **Industry Agnostic Data Loss Prevention (DLP) solutions, and industry-specific technology solutions:** providing software that detects, identifies, monitors, and controls sensitive data leaving a network.

Each of these systems play their part in the incident response process, coming together to provide the detection, tracking and analysis of privacy and security events.



The ecosystem of detection, analysis, monitoring, and management systems are effective at identifying security and privacy events, but don't provide guidance on whether such an event rises to the level of a notifiable breach under state or federal laws.

I've Detected an Incident...Now What?

These tools are excellent for knowing when an incident has taken place, but what happens when the security or privacy incident involves the exposure of regulated data? At the end of the day, after the detection and tracking of an event, privacy and security teams find themselves on their own in determining if an event is notifiable, and if so, which state, federal and regulatory bodies require notification — and by when?

Enter RadarFirst, a innovative SaaS-based incident response management platform, that automates and simplifies assessment of privacy and security incidents, ensuring compliance with federal and state breach laws. RadarFirst

complements the security and privacy incident management ecosystem and is designed to close the loop on incident response, taking the information gathered in privacy and security systems and providing the next step: guidance to determine if an incident is a breach, whether it is notifiable, which regulatory bodies must be notified, and by what date.

How RadarFirst Works

The RadarFirst Breach Guidance Engine™ leads users through an intuitive workflow that profiles and scores data privacy and security incidents and generates incident-specific notification guidelines to help ensure compliance with federal and state laws.

Step-by-step guidance: The RadarFirst Breach Guidance Engine™ and purpose-built workflow guides users through a process for profiling and scoring any data privacy or security incident to determine whether the incident is a data breach.

Automated plan for response: the RadarFirst assessment generates an incident-specific response plan and notification guidance according to relevant data breach notification laws (including GDPR), along with required documentation to support an organization's burden of proof obligation under breach laws.

Reliable and up-to-date: RadarFirst is current with federal, state, and international data breach regulations — including GDPR.

SaaS Solution for Integrated Systems

The RadarFirst platform is offered as a SaaS application, which is critical to keeping our solution up-to-date with constantly changing state and federal breach notification laws.

As a means to complement the detection and management of incidents identified through existing security and privacy tools, RadarFirst provides a REST API that allows clients to automate the creation of incidents in RadarFirst for risk assessment and regulatory guidance.

RadarFirst's Privacy and Security Certifications

RadarFirst has been issued a SOC 2 Type II report, a comprehensive certification demonstrating the ability to keep sensitive data secure. RadarFirst has also certified with the Privacy Shield Framework, signifying our commitment to comply with EU data protection requirements when transferring personal data between the United States and the European Union in transatlantic commerce.

[Request a Demo](#)

Example RadarFirst assessment, showing jurisdiction and incident-specific regulatory guidance based on data sensitivity and incident severity.

The screenshot displays two assessment panels for Connecticut and Florida. Each panel includes a data sensitivity matrix, a table of notifications, and specific guidance messages.

Connecticut Assessment:

- State: Connecticut (High)
- Decision: Pending
- Matrix: Data Sensitivity (High, Medium, Low) vs Incident Severity (Low, Medium, High, Severe). High severity with high sensitivity is red.
- Notifications Table:

Name	Guidance	Decision	Due	Notified
Affected Individual	Yes	Yes	10/2/18	not specified
Attorney General	Yes	Yes		not specified
Connecticut Attorney General	None	not specified	10/2/18	

- Buttons: Regulated data, Law overview, Get firm decision.

Florida Assessment:

- State: Florida (High)
- Decision: Pending
- Matrix: Same as Connecticut.
- Guidance messages: "The state law provides the following exemptions. If these exemptions apply to your entity, you can override RadarFirst's guidance to take advantage of applicable exemptions..."
- Notifications Table:

Name	Guidance	Decision	Due	Notified
Affected Individual	Yes	Yes	10/2/18	not specified
Attorney General	No	No	10/2/18	

- Buttons: Regulated data, Law overview.



Learn more at radarfirst.com

RadarFirst's award-winning incident response management software is trusted by organizations in heavily regulated industries to reduce risk and simplify compliance with global data breach laws.