RadarFirst

AUTOMATING INTELLIGENT DECISIONS

Reduce risk. Simplify obligation decision-making. RadarFirst is the SaaS solution to:

- Leverage automation to reduce time to incident resolution and ensure consistent, documented obligation decision-making
- Stay current with ever-evolving laws, rules, and regulations
- Protect brand reputation and mitigate risk associated with incidents and potential breaches
- Prepare accurate and timely reports for internal stakeholders and external auditors
- Operationalize documentation associated with event assessments
- Ensure compliance with both regulatory and third-party contractual notification obligations

Trusted by Privacy, Cyber & Compliance Teams

"We've transitioned to a digital-first company, with all of our in-house data centers in the cloud. Radar® Privacy offers an innovative and secure SaaS solution, ideal for our current and future compliance needs."

-Privacy Officer

"Radar® Compliance allows us to better uphold our culture of compliance. We can decide to notify regulators as recommended or even more often to maintain good relations."

-Multinational Compliance Officer

"Radar® Privacy provides consistent guidance for a growing volume of privacy and security incidents reducing our compliance and reputational risk."

-Executive Compliance Officer

"When you think about corporate entity-level risk matrices, Radar® Compliance gives us a predefined structure and a consistent path that can be presented to our Board and regulators."

-Multinational Compliance Analyst

"All of the regulatory requirements around breaches, notifications, and deadlines are built right into Radar® Privacy. This created an easy workflow that's saved at least 50% of the time it takes to complete assessments."

-Global Privacy Lead

"What I do for a living is litigation avoidance. For us, RadarFirst answers the questions of how do we do what we need to do, do the right thing by the people and groups who are impacted, but also do it in a way that protects us from regulatory fines and assessments and keeps us out of third-party class action lawsuits."

-Deputy Privacy Officer

Capital One | Aflac | UnitedHealth Group | USAA | Humana

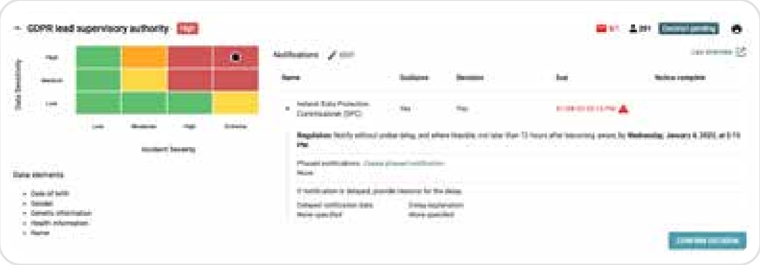
Raymond James | Pacific Life | Lincoln Financial Group | motorola

Solutions for Evolving Regulations

With patented Radar® technology, organizations can define, streamline, and scale decision-making against time bound notification requirements supported by consistent, objective processes with documented outcomes.

Built on the award-winning **Radar® platform**, organizations can operationalize Cyber, Compliance, Risk, Privacy, internal, and third-party notification obligations with any combination of our two SaaS solutions.

Radar® Privacy is custom built to assess harm to individuals, and is the global standard for documentable and consistent privacy incident management, offering intelligent decision support for assessing privacy incidents against global breach notification laws.



Notifications

Name	Guidance	Decision	Due	Notice complete
Ireland Data Protection Commissioner (DPC)	Yes	Yes	[illegible]	

Regulation: Notify without undue delay and where feasible not later than 72 hours after becoming aware by **Wednesday, January 4, 2023, at [illegible] PM**

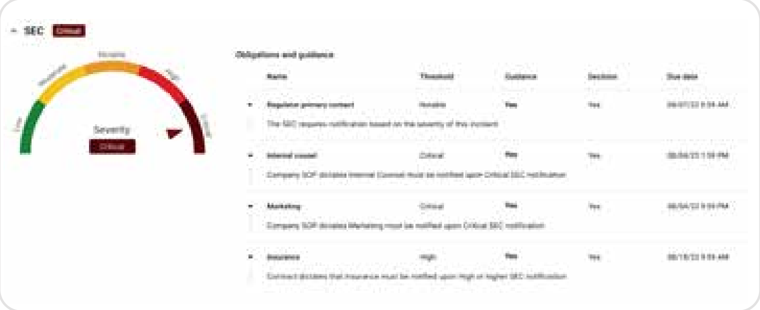
Phased notifications: Create phased notification
None

If notification is delayed, provide reason for the delay.

Delayed notification date: None specified
Delay explanation: None specified

Data elements
- Date of birth
- Gender
- Genetic information
- Health information
- Name

Radar® Compliance provides a fully configurable rules engine that ingests company-specific risk ratings and severity levels to to consistently evaluate the severity of event, its potential harm to the organization, and the company's obligations to notify to both internal and external stakeholders, such as SEC regulators and/or the Board of Directors.



Obligations and guidance

Name	Threshold	Guidance	Decision	Due date
Regulator primary contact	Notable	Yes	Yes	08/07/23 9:59 AM
The SEC requires notification based on the severity of this incident				
Internal counsel	Critical	Yes	Yes	08/04/23 1:59 PM
Company SOP dictates Internal Counsel must be notified upon Critical SEC notification				
Marketing	Critical	Yes	Yes	08/04/23 9:59 PM
Company SOP dictates Marketing must be notified upon Critical SEC notification				
Insurance	High	Yes	Yes	08/18/23 9:59 AM
Contract dictates that insurance must be notified upon High or higher SEC notification				

Radar® Platform Capabilities

- **Privacy Incident Decision Intelligence:** Patented automation that considers all relevant privacy incident risk factors and programmatically analyzes risk of harm to individuals against applicable data breach laws and regulations, accelerating time to breach resolution.
- **Event Risk Assessments:** Configurable cyber, compliance, and risk event assessment engine to determine potential harm to an organization based on company-identified risk factors, and the necessary notification obligations to mitigate identified risk.
- **Third-Party Notifications**: Consideration of third-party contractual notification obligations in addition to applicable laws and regulations during the risk assessment of an incident.
- **Multiple Incident Dimensions**: Complex incidents typically touch multiple departments (e.g., security, privacy, compliance) and require consolidated communication for all impacted teams. Facilitate cross-department collaboration within the Radar® platform to unify incident management activities.
- **Privacy Benchmarking Metrics**: Analysis of aggregated and anonymized data to generate comparative incident management metrics that benchmark your organization across the industry and with peers.
- **Global Breach Law Library**: Up-to-date library of global data breach laws mapped to an automated risk assessment, including regulatory watchlists that track proposed and recently passed legislation.

Radar® Privacy

Intelligent Incident Response

Challenge: How can privacy teams, stretched thin by an ever-evolving and complex privacy landscape, quickly and consistently determine whether or not a breach is notifiable?

Solution: Radar® Privacy is the decision support platform to simplify notification decision-making and decrease time to incident resolution.

To meet compliance requirements and avoid costly regulatory or reputational penalties, privacy professionals must race to determine if an incident requires notification. This requires teams to navigate a landscape of ever-changing regulations, new deadlines, and varying definitions of personal information (PI).

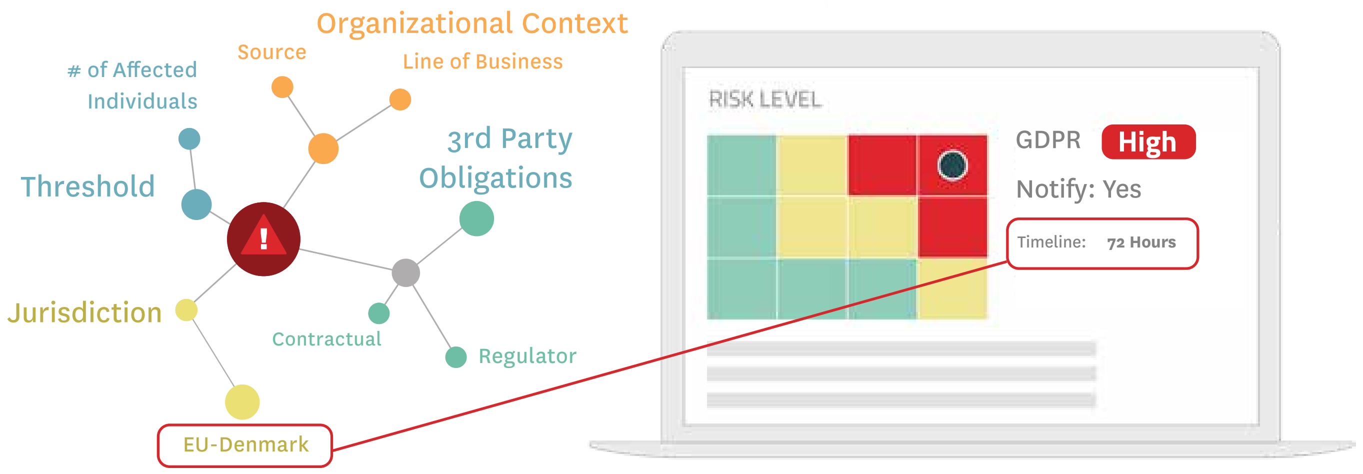
With so much complexity to account for, making objective data breach notification decisions within regulatory and contractual timeframes is challenging—but essential for organizational risk management.

Radar® Privacy's custom-built data breach notification decision-support engine maps all current state, federal, global, and contractual notification obligations to an automated risk assessment, giving you detailed and consistent incident risk scoring, regardless of how convoluted the regulatory or PI details.

Additionally, once a decision to notify is made by the organization, Radar® Privacy provides all the notification requirements and timelines under applicable international and U.S. laws, creating greater efficiency and reducing risk of non-compliance.

Key Solution Benefits

- **Simplify compliance with current data breach notification laws** via the patented Radar® Breach Guidance Engine
- **Ensure consistent and accurate automated risk assessments**
- **Streamline the complete lifecycle of an incident,** from discovery and investigation to assessment and notification decision
- **Increase efficiency** by enabling cross functional departments to work in concert to quickly resolve multi team incidents
- **Perform analysis of benchmarking data** to identify trends and areas for improvement and risk mitigation
- **Satisfy complex audit and reporting obligations** by storing all incident assessment documentation, breach notification decisions, reports, and audit logs in one location



Radar® Compliance

Operationalize SEC Compliance

Challenge: Cyber event obligations are becoming more strict and punitive—and at the same time less well-defined. Additionally, regulators are insisting on clearly documented evidence that a “materiality” risk assessment was performed as part of the notification obligation decision-making process.

Organizations need a flexible, scalable, and configurable notification management solution to ensure compliance—and risk mitigation—in today’s complicated regulatory landscape.

The Solution

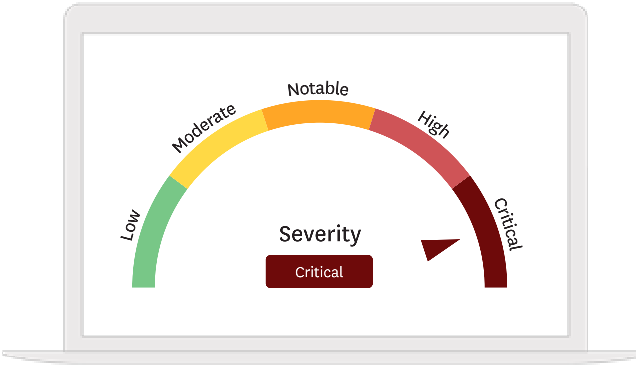
Radar® Compliance is a configurable rules and assessment engine that offers organizations the ability to define their own notification triggers and obligations to stakeholders, from federal regulators to the board of directors.

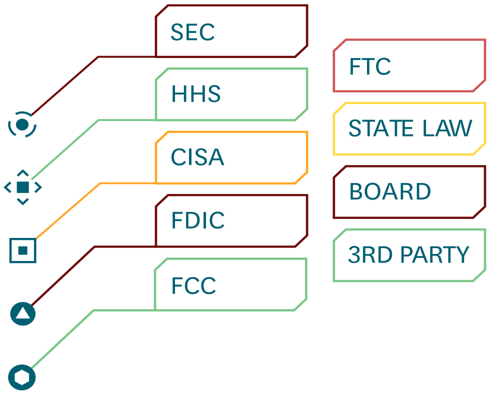
Custom-built for flexibility, Radar® Compliance is able to address a wide variety of incidents, including but not limited to cyber events, health and welfare, operational interruptions, and internal compliance. And when an incident involves personal information (PI), Radar® Privacy can seamlessly operate within the context of the same incident to further streamline the incident workflow process and reduce time to event resolution.

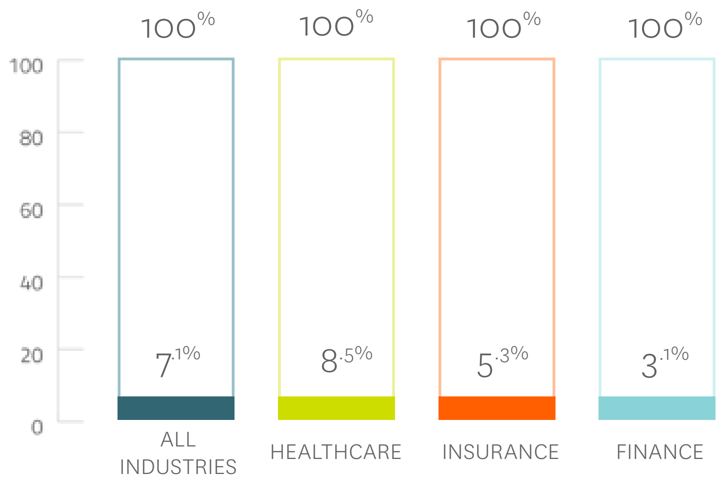
Organizations can be confident that they not only fulfill event notification obligations to each and every internal and external stakeholder but, critically, also meet the regulatory need for detailed and consistent documentation.

Key Solution Benefits

- **Consistent and detailed risk assessment** eliminates subjectivity inherent in manual approaches for assessing an incident against a risk matrix. Ad hoc notification decisions will be a thing of the past.
- **Proof of compliance**, i.e. audit trails, provide a transparent process to internal and external stakeholders; the solution offers the inherent traceability and defensibility that every organization subject to a regulator needs.
- **Elimination of over and under incident reporting**, potentially reducing fines leveraged by regulatory bodies.
- **Increased controls** that simplify record keeping and create streamlined, documentable processes.
- **Reduction of fines** and decreased instances of enforcement actions leveraged due to poor controls.
- **Customizable to fit a company’s unique culture of compliance and risk** via the ability to create rules based on a business case unique to the organization, and specific to their definition of material harm.







Organizations without automation presume all incidents are a notifiable breach

With automation in place, on average, organizations report only **7% of data breaches**

The Risks of Over-reporting

Over-reporting can erode the confidence that customers have in your brand, and your ability to protect their privacy. If you continue to over-report breaches, your customers may wonder just how secure your business really is. And that can cost you a lot.

An Accenture Strategy Research Report found that trust, traditionally viewed as a "soft corporate issue," has a very real impact on the bottom line.

In fact, at least **$180 billion in revenue** is at stake across the **54% of companies** in the Accenture analysis that experienced a drop in trust.

The Risks of Under-reporting

By missing notification requirements, and therefore under- reporting, organizations open themselves up to risk of significant fines and penalties. As an example, Altaba, formerly known as Yahoo!, agreed to pay a $35 million penalty for failing to disclose its massive cybersecurity breach to investors. Failing to notify diminishes consumer confidence and thus can take a financial toll.

Regarding the trust issue, Michael Lyman, senior managing director at Accenture Strategy, said,

"Our research proves that no company is immune to the impact of a drop in trust on the bottom line. U.S. companies must adopt a top-down culture that fully bakes trust into the company's strategy, operations and broader DNA. Those who don't are putting their future revenues at risk."

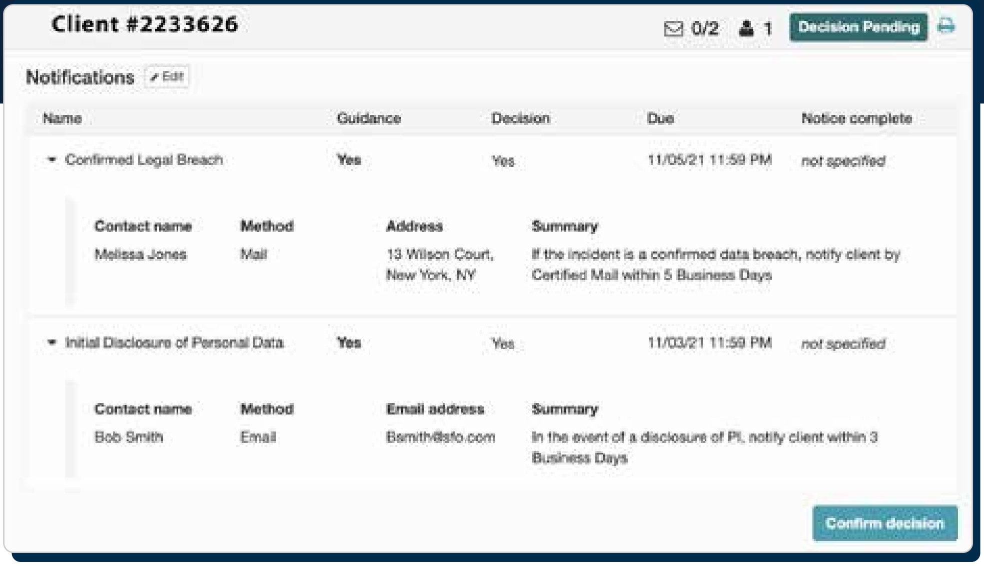
Over-reporting Leads to:

- **Brand and reputational damage**
- **Erosion of confidence from general public**
- **Greater regulatory scrutiny**
- **Increased operational costs**

Under-reporting Results in:

- **Fines and penalties**
- **Diminished consumer confidence, resulting in impacts to the bottom line**
- **M&A implications**

RadarFirst | Third-Party Notification Module



Client #2233626

Notifications

Name	Guidance	Decision	Due	Notice complete
Confirmed Legal Breach	Yes	Yes	11/05/21 11:59 PM	*not specified*

Contact name	Method	Address	Summary
Melissa Jones	Mail	13 Wilson Court, New York, NY	If the incident is a confirmed data breach, notify client by Certified Mail within 5 Business Days

Name	Guidance	Decision	Due	Notice complete
Initial Disclosure of Personal Data	Yes	Yes	11/03/21 11:59 PM	*not specified*

Contact name	Method	Email address	Summary
Bob Smith	Email	Bsmith@sfo.com	In the event of a disclosure of PI, notify client within 3 Business Days

Close the Loop on Regulatory and Contractual Incident Response and Notification Obligations

RadarFirst's Third-Party Notification module tracks if your upstream and downstream entities remain compliant with contracts, so you may identify risk to your business. Alongside the contractual obligations, Third-Party Notification allows you to easily scan and prioritize your data breach response.

Until now, managing third-party notifications has been a manual, time-consuming process that requires sifting through contracts, and creates risk of noncompliance. Contractual notification obligations are often measured in hours or days rather than weeks or months, providing a major challenge to compliance. Noncompliance can result in serious consequences, including termination of relationships if obligations are not satisfied.

Third-Party Notification Module

For managing upstream notification obligations to your clients, the Radar® platform seamlessly extends its regulatory workflow to identify and provide guidance on all relevant incidents involving client data and third-party notification requirements.

You can take advantage of a fully integrated workflow to manage all regulatory and third-party incident response obligations, prove compliance, and mitigate risks stemming from incidents involving your own data or data that you process for your clients.

Optimize Cross-Functional Collaboration

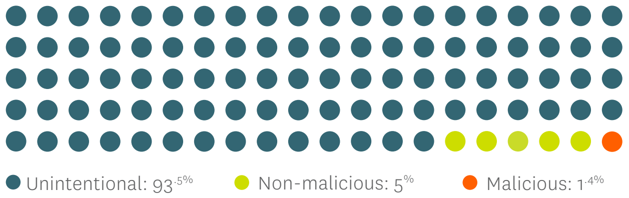
- **Efficiently manages your third-party notification obligations** with clients or upstream entities (who you must notify)
- **Effectively monitors compliance by your service providers or downstream entities** (who must notify you)
- **Uses the Radar® Breach Guidance Engine to assess the risk** associated with an incident, and determine whether one or multiple clients must be notified
- **Captures important contractual notification details for each external entity**, including multiple notification timelines and contacts
- **Provides easy tracking** of notification due dates and proof of compliance with contractual obligations
- **Allows for a nuanced configuration** in which downstream entities act as an agent of your organization, to more accurately specify the correct incident discovery date

RadarFirst

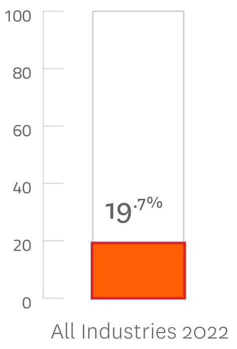
KPIs to Reduce Risk

In the digital age, breaches have become a costly and unavoidable reality for all companies that collect and manage data. To remain competitive, organizations must not only collect data but also leverage third-party relationships to better serve and understand their customers. However, each new partnership invites risk. The question is when – not if – a data breach will occur. When it does, having an incident management solution in place is critical. ***Here's What RadarFirst Can Do.***

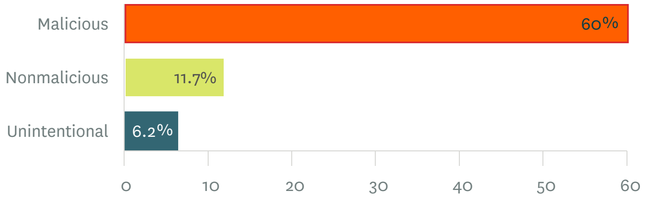
Find the # of notifiable incidents happening in your organization



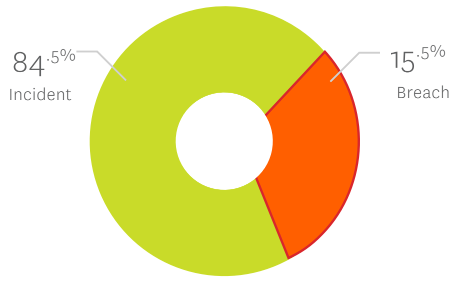
Identify the percentage of overdue notifications



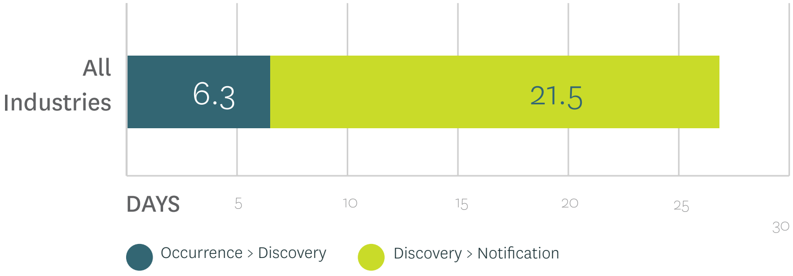
Pinpoint notifiable incidents by intent



Analyze downstream third-party breaches



Calculate how long it takes your team to Discover and Notify



RadarFirst

The Bottom Line

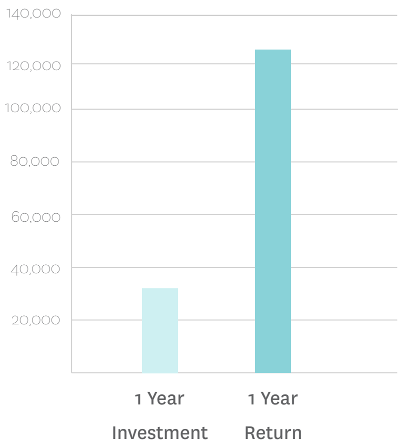
RadarFirst offers the world's only end-to-end risk management solution. If trust is the currency of modern business, RadarFirst is the insurance. With Radar® Privacy and Radar® Compliance you can solve the most complex challenges of incident management within seconds using patented, intelligent automation. Transform your risk management processes and learn why RadarFirst boasts a **99% customer retention rate**.

Only RadarFirst Can Generate:

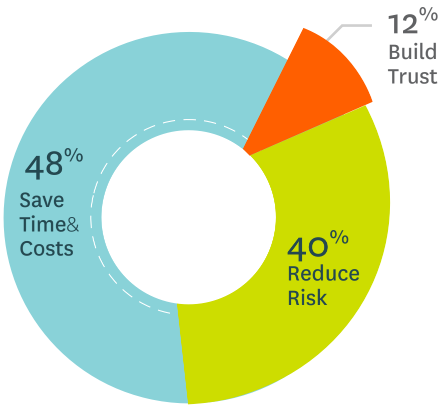
ROI Analysis

3-Year ROI	274%
3-Year NPV	$88,739
Payback (months)	3.2
Investment - Year 1	$35,600

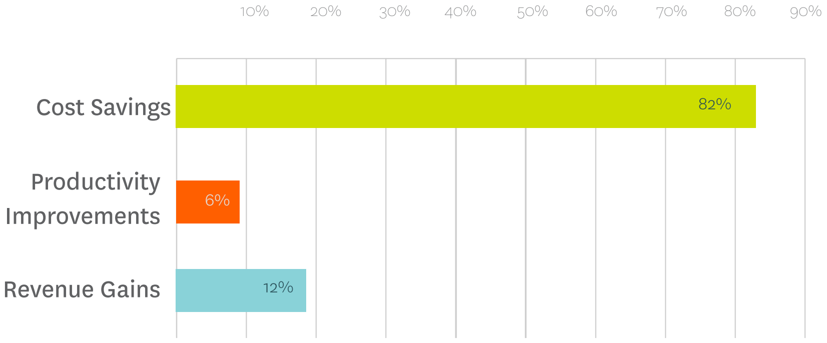
ROI Timeline



Benefits by Value-Driver



Benefits by Type



RadarFirst

Additional Resources

[Industry Report] 2024 Privacy Incident Management Benchmarking Report

Learn more »

radarfirst.com/2024-benchmarking

[Datasheet] The True Cost of Office Productivity Tools

Learn more »

radarfirst.com/true-cost

[Guide] Risk Reporting Maturity Level Guide

Learn more »

radarfirst.com/risk-reporting

RadarFirst

WINNER
The HPE-IAPP
Privacy Technology
Innovation Award
iapp

AICPA Service Organization Control Reports
AICPA
SERVICE ORGANIZATIONS
SOC
aicpa.org/soc
Formerly SAS 70 Reports

About RadarFirst

RadarFirst offers SaaS solutions trusted by enterprises and organizations to reduce risk and simplify legal governance, risk, and compliance (GRC) incident management. The award-winning Radar® technology automates assessment processes to help companies meet time-bound response requirements and delivers transparent notification obligation decision-making against global data breach laws, as well as compliance and cyber regulations. With RadarFirst, organizations can define, document, and scale decision-making in a consistent, objective process.

Learn more at radarfirst.com.