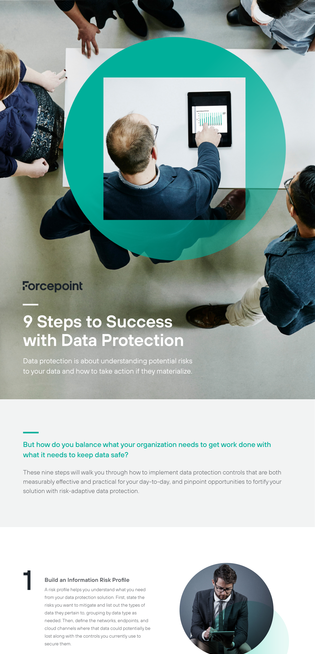


Forcepoint

9 Steps to Success with Data Protection

Data protection is about understanding potential risks to your data and how to take action if they materialize.

But how do you balance what your organization needs to get work done with what it needs to keep data safe?

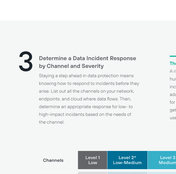
These nine steps will walk you through how to implement data protection controls that are both measurably effective and practical for your day-to-day, and pinpoint opportunities to fortify your solution with risk-adaptive data protection.

1 Build an Information Risk Profile

A risk profile helps you understand what you need from your data protection solution. First, state the risks you want to mitigate and list out the types of data they pertain to: grouping by data type as needed. Then, define the networks, endpoints, and cloud channels where that data could potentially be lost along with the controls you currently use to secure them.

2 Create a Data Incident Severity and Response Chart

Mapping each data type to its business impact will allow you to prioritize your responses and keep security resources focused where they're most effective. For some organizations, this can be a challenging exercise. To start, sit down with data owners to discuss which types should be protected and what's at risk should they be compromised. Then, rank each on a scale of 1-5 (1=low impact, 5=high impact) and define an acceptable response time for each according to the severity of the risk—you'll want to secure the high-risk data types first.



The Risk-adaptive Difference:

Risk-adaptive data protection is designed to prioritize high-risk activity, autonomously enforce controls based on risk, and reduce the time it takes to investigate an incident.

3 Determine a Data Incident Response by Channel and Severity

Staying a step ahead in data protection means knowing how to respond to incidents before they arise. Lay out all the channels on your network, endpoints, and cloud where data flows. Then, determine an appropriate response for low- to high-impact incidents based on the needs of the channel.

The Risk-adaptive Difference:

A risk-adaptive solution accounts for the risk level of every human who touches your data, empowering you to adjust incident responses based on individual risk. For example, adapting response to audit-only for low-risk users and block for high-risk only ensures that every member of your team can get the work done without compromising data or impacting user productivity.

Channels	Level 1 Low	Level 2* Low-Medium	Level 3 Medium	Level 4* Medium-High	Level 5* High	Notes
Email	Encrypt	Drop Email Attachments	Quarantine	Quarantine		Encryption
Web						Proxy to Block
Secure Web						SSL Inspection
FTP	Audit	Audit/Notify	Block/Notify	Block/Alert	Block	Proxy to Block
Network Printer						Install DLP Printer Agent
Custom						
Cloud Applications			Quarantine with Note	Quarantine		

* Additional granularity available with risk-adaptive data protection.

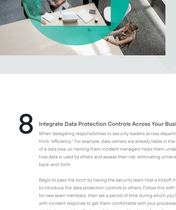
4 Establish an Incident Workflow

Ensure that your security teams can jump into action the moment an incident is detected by clearly defining the response workflow for low- to high-impact incidents. For lower-impact incidents, automate wherever possible. This will free up bandwidth for hands-on remediation of higher-impact incidents.

The Risk-adaptive Difference:

A risk-adaptive solution lets you analyze incidents based on individual risk level, without needing to engage an incident analyst to determine the best action to take. Incidents tied to low-risk individuals may not pose a threat to your business, so allowing them to carry on (with added safeguards such as encryption for USB file transfer or automatically dropping email attachments) can keep the wheels of productivity turning.

Administrators can take the same proactive approach with high-risk people and incidents by automatically blocking or restricting specific actions until an incident analyst can investigate.



5 Assign Roles and Responsibilities

Forrester data protection program stability, scalability, and operational efficiency by defining who's who on your team. Assign key roles such as technical administrators, incident analysts, forensics investigators, and auditors and bestow the proper rights and access to each.

6 Begin Project in Monitoring Mode

Once you have your network data protection solution in place, a monitoring period will let you identify patterns in your activity and set a baseline to help you recognize normal user behavior. Once this period is complete, analyze the behavior you've observed and present your findings to your executive team, along with recommendations for how to mitigate risks. You can then put those recommendations into action, monitor their success, and present to your executives again.

The Risk-adaptive Difference:

With a risk-adaptive solution, analyzing incidents in audit-only mode (as opposed to preloaded enforcement mode) will highlight the reduction of incidents requiring investigation—without compromising your data. Plus, you'll observe more positive incidents without stretching resources to address false threats.

7 Move to Proactive Protection

What you've learned in monitoring mode will give you the level of confidence you need to transition into blocking mode for high-risk events, or in accordance with your incident response plan. As you deploy data protection to endpoints and sanctioned cloud applications, you'll monitor, analyze, report, optimize, and re-report your findings to the executive team.

8 Integrate Data Protection Controls Across Your Business

When delegating responsibilities to security leaders across departments think "efficiency." For example, data owners are already table in the event of a data loss, so naming them incident managers helps them understand how data is used by others and lessens their risk, eliminating unnecessary back-and-forth.

Begin to pass the torch by having the security team host a kickoff meeting to introduce the data protection controls to others. Follow this with training for new team members, then set a period of time during which you'll assist with incident response to get them comfortable with your processes. You might also consider offering real-time coaching to reinforce those processes.

9 Track the Results of Risk Reduction

You started to set yourself up for this in Step 6—here's what's left. Group relative incidents together by criteria such as severity, channel, data type, and regulation. Then, set your Monitoring and Risk Reduction periods to be of equal length (try two weeks each to start) to preserve the integrity of your results.

Likelihood of Data Loss

Number of Incidents over 90 Days

Incidents	Week 1	Week 2	Week 3	Week 4	Percent Reduction
30 days baseline	100	100	100	100	0%
60 days (30 days monitoring)	100	100	95	90	10%
90 days (60 days monitoring)	95%	90%	85%	80%	20%
90 days (90 days monitoring)	75%	60%	50%	40%	60%

Goals

30 days	90 days
20% reduction	50% reduction

The Risk-adaptive Difference:

With a risk-adaptive approach, you'll want to provide a comparison of the incidents captured in audit-only mode (all incidents) versus incidents requiring investigation with graduated enforcement. The summary should show the number of incidents for each risk level 1-5, contrasted against those actually requiring investigation (risk levels 4-5).

Whether you take a traditional approach or augment your security with risk-adaptive data protection, this proven formula will help guide you to success.

Forcepoint

Want to see risk-adaptive protection in action?

See it Here