cyberhaven

The 15 Top Data Detection and Response Use Cases

What is Data Detection and Response?

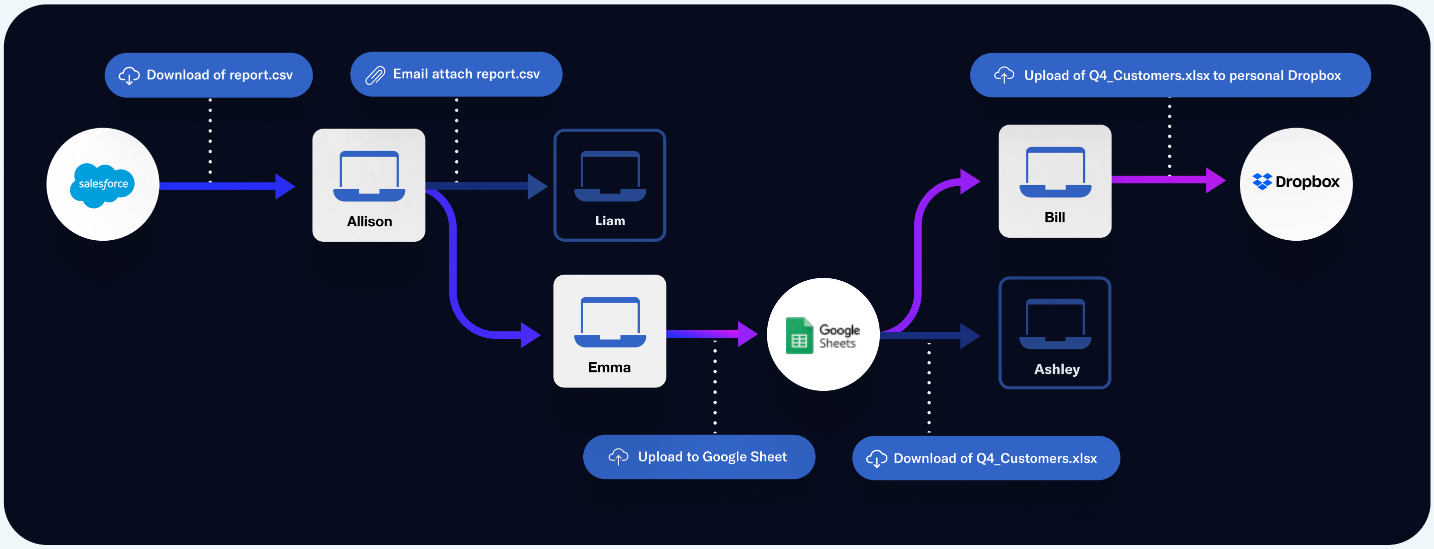
Data detection and response (DDR) is a transformational data security technology that makes it possible for companies to better protect their data from insider threats and accidental exposure.

Today, companies rely on a combination of data loss prevention (DLP), insider risk management (IRM), cloud access security broker (CASB), and user and entity behavior analytics (UEBA) tools to address this risk – but none have fully solved the problem.

By addressing use cases that these legacy tools attempt to serve and addressing their shortcomings, DDR provides a single platform that results in more robust data security that's less of a burden to deploy and manage.

Data Tracing - The Magic Behind Data Detection and Response

The heart of DDR is data tracing, which analyzes billions of events related to all pieces of data. It continuously creates and updates the entire lineage of any piece of data within your organization from its creation onward to better classify and protect it.



Rather than relying entirely on content inspection to classify what type of data it is, DDR also collects every event and interaction with every piece of data across your managed devices, browsers, and your cloud applications.

For every piece of data, tracing tells you:

1. Where it came from
2. Who interacted with it
3. How it was handled

This contextual information enables DDR's superior approach to the use cases below.

What You’ll Learn in this Guide

In this guide, you’ll learn how DDR helps companies:

Stop exfiltration of sensitive data

1

Prevent sensitive data from leaving by enforcing blocking across all major exfiltration channels

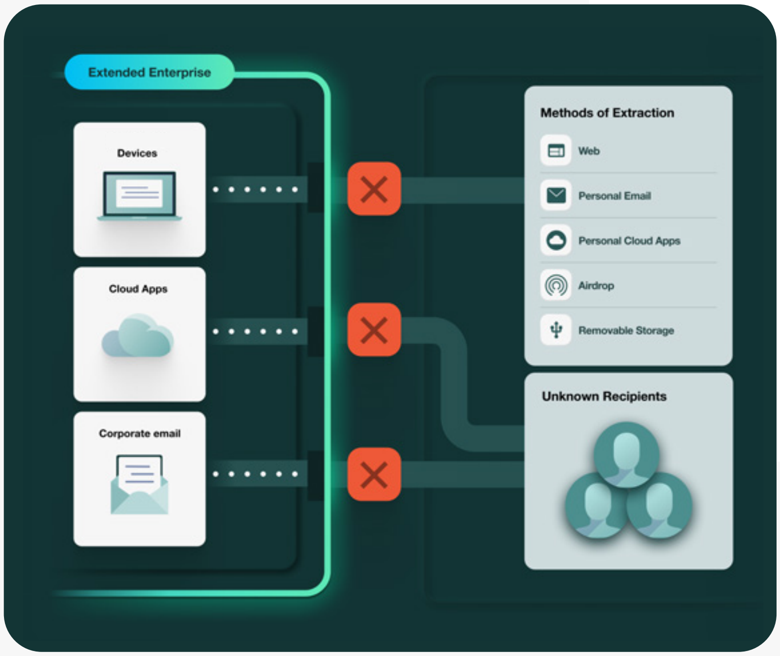
Detecting risks to data isn't enough, you have to stop data exfiltration. Until now, companies have had to rely on different tools to protect different egress channels. DDR makes it possible to stop exfiltration across all channels with one product and one set of policies.

Functional Requirements

✓ A single product, single place to manage policies, and single remediation workflow for all exfiltration channels

✓ Block egress via all major exfiltration methods:

- Direct sharing from corporate cloud applications
- Direct emails from corporate email
- Web uploads
- Personal email
- Personal cloud applications
- Bluetooth and AirDrop
- USB and other external storage



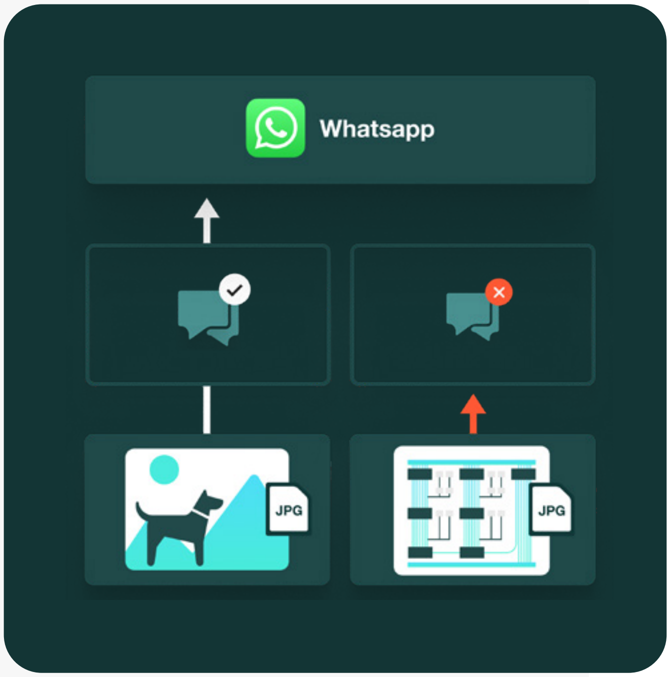
2

Classify data that doesn’t contain a content pattern or contains no text

Other solutions rely solely on content inspection to identify different types of sensitive data (e.g. credit card numbers, Social Security numbers). This makes it almost impossible to classify data that contains no consistent content pattern (e.g. customer documents, design files) or no text at all (e.g. recorded meetings, pre-launch marketing images). DDR utilizes the context captured by data lineage to overcome this challenge.

Functional Requirements

CLASSIFICATION	EXAMPLE
Classify data based on **where it originated**	Product designs originated from Figma
Classify data based on **how it was handled**	Presentation files in the board meeting prep site in Sharepoint
Classify data based on **who interacted with it**	Drug formulas developed by the research team



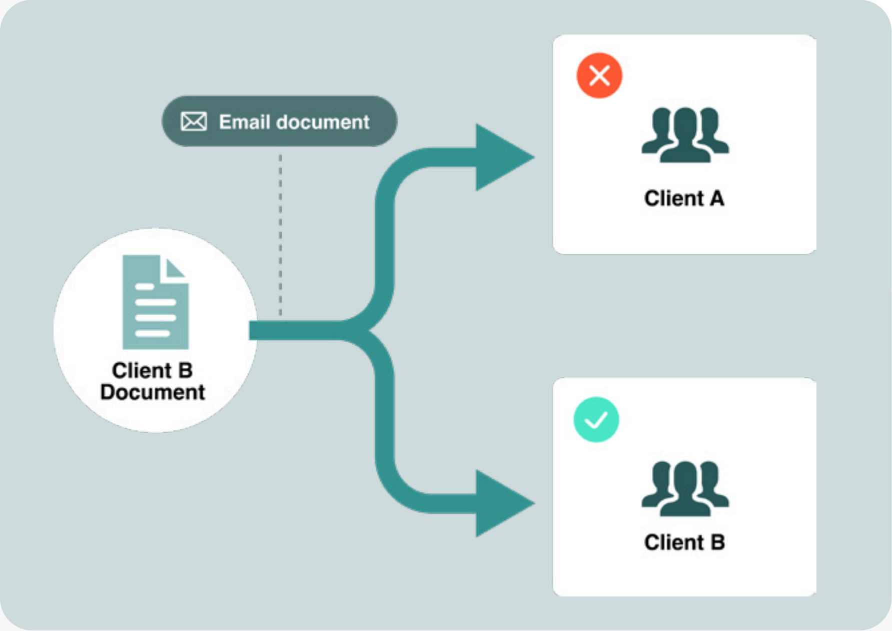
3

Ensure client documents are never shared inappropriately

When working with customers, mistakes happen. A single misclick can result in the wrong document getting attached or the wrong recipient being selected. DDR and data lineage gives organizations granular control over data movement to prevent these kinds of mistakes.

Functional Requirements

- ✓ Identify data as belonging to a specific customer
- ✓ Identify the recipient as the customer or someone else
- ✓ Block movement of customer data outside a defined set of employees and the customer themselves



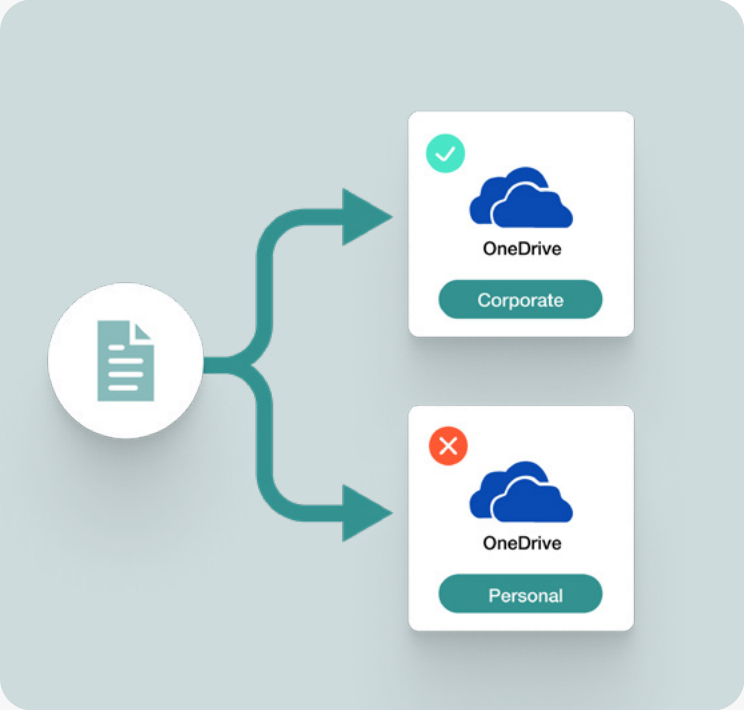
4

Enforce different policies for corporate and personal instances of the same app

It's one thing to stop sensitive company data going to personal cloud storage services. It gets trickier when an employee has a personal instance of the same application that the company allows (even encourages) employees to use for important data. DDR can enforce a different policy for each (e.g. allow financial data to go to corporate OneDrive but not someone's personal OneDrive)

Functional Requirements

- ✓ Distinguish between corporate and personal instances of the same application
- ✓ Enforce policies selectively on personal versions of applications



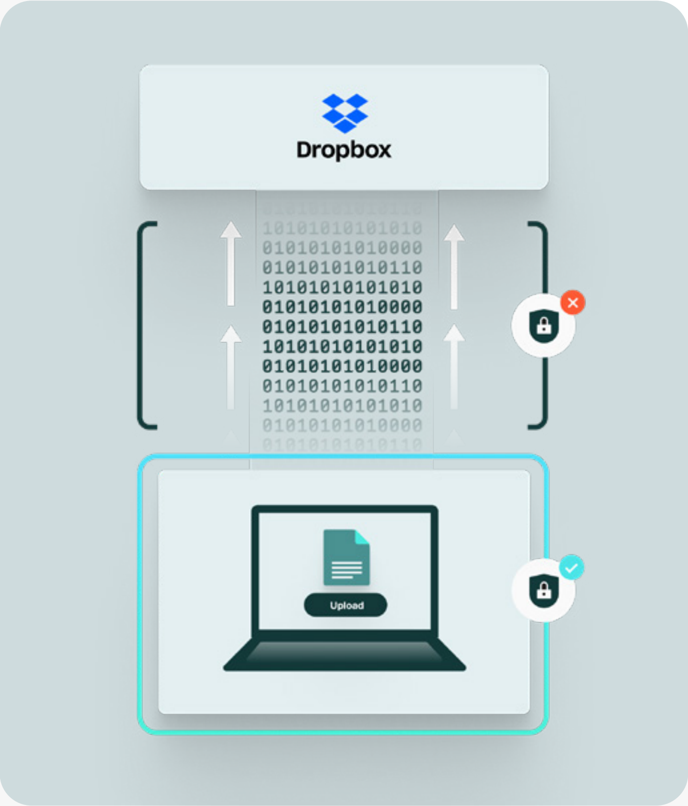
5

Understand and control usage of certificate pinned and end-to-end encrypted applications

Advances in network security have resulted in two approaches to better secure data in transit – certificate pinning and end-to-end encryption. However, these approaches have rendered CASB and web proxy approaches to data security completely ineffective on commonly used applications like Dropbox and Whatsapp. By enforcing controls on the device itself, DDR can protect data before visibility is lost.

Functional Requirements

- ✓ Inspect activity and data to and from the cloud on the device before it's encrypted and after it's decrypted
- ✓ Ability to block risky behavior in real time



Understand data movement

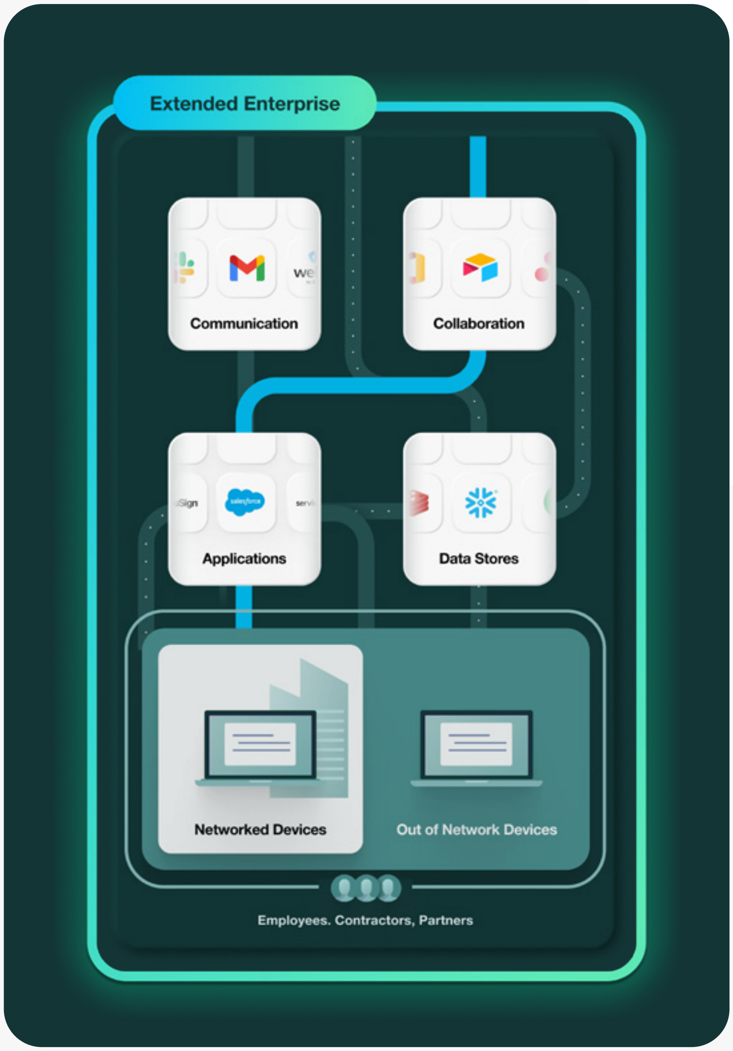
6

Understand the sprawl of sensitive data

There's a lot of focus on limiting access to data in different systems. But data has a tendency to move and flow through the organization as it is shared, downloaded, uploaded, copied, etc.. Through the process of everyday collaboration it reaches people who don't have access to it at the source. This sprawl increases risk to sensitive data as more people have copies of it and DDR makes it possible for the first time for companies to understand this sprawl.

Functional Requirements

- ✓ Track every data copy and derivative as it moves through the organization
- ✓ Filter data movement by type of data, sensitivity, risk level
- ✓ Identify what systems are being used to store sensitive data
- ✓ Identify which employees have copies of sensitive data



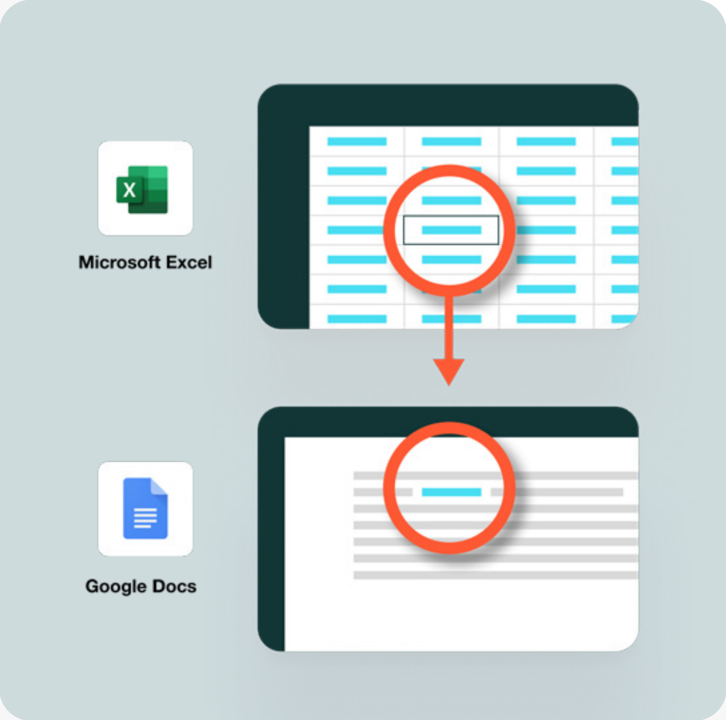
7

Track and protect sensitive data copied between files or apps

Many data security products focus on data in files. They scan content in files and apply tags/labels to files. But what happens when data is copied out of the file? And what about the significant and growing amount of data that is never contained in a file at all, it's just in an application. DDR operates at a more granular level, tracking and protecting every piece of data.

Functional Requirements

- ✓ Track every piece of data at the most granular level across files and applications
- ✓ Maintain classification of each piece of data without relying on tagging or modifications to the data



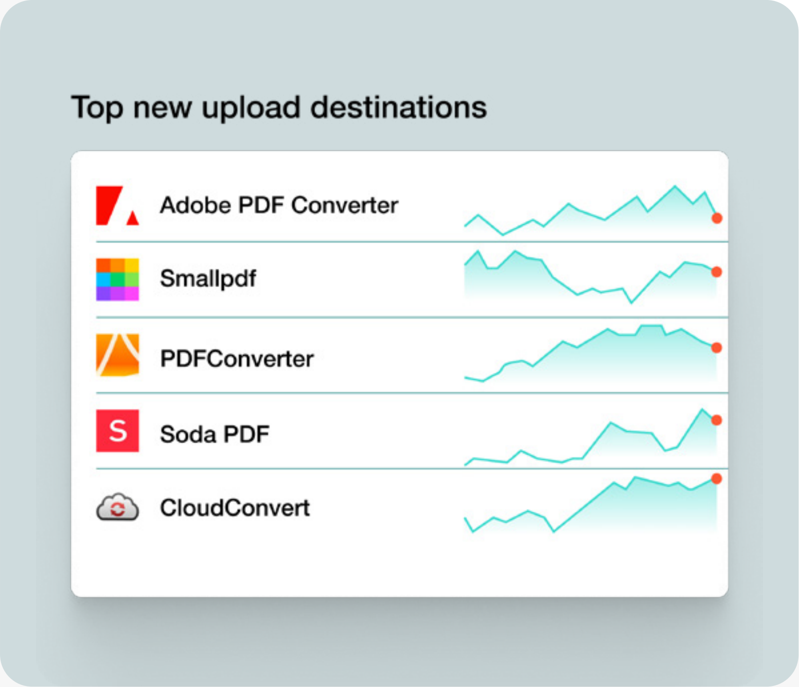
8

Discover cloud applications and data stores that are actively used

Modern IT environments are a complex, fast-evolving web of applications and data stores. Understanding where sensitive data lives and ensuring proper controls requires a large manual effort on the part of security teams using legacy solutions. DDR automatically detects and tracks usage of new cloud apps employees try to use with company data.

Functional Requirements

- ✓ Track all data uploaded and downloaded from cloud applications
- ✓ Query and visualize all destinations and sources of sensitive data



Top new upload destinations

Adobe PDF Converter

Smallpdf

PDFConverter

Soda PDF

CloudConvert

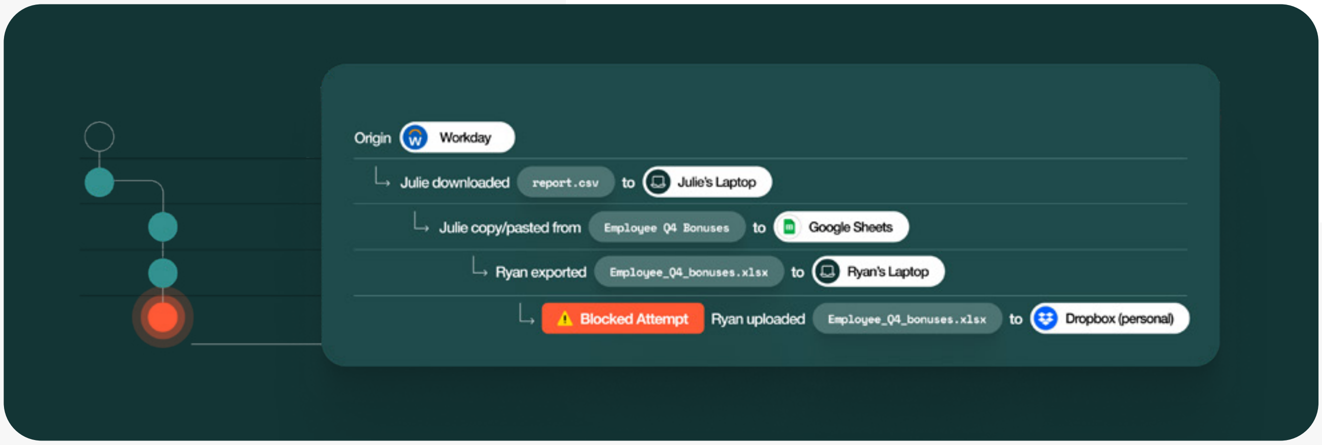
9

After an incident, determine how someone got access to data they can't access at the source

Part of incident response to a data leak is determining the root cause to update policies and strategies to reduce risk. With data lineage, DDR turns a weeks-long process of investigation into a matter of hours.

Functional Requirements

- ✓ Track every data copy and derivative as it moves through the organization
- ✓ Visualization of complete data lineage showing how it moved through the company to the person who mishandled it



Origin Workday

↳ Julie downloaded `report.csv` to Julie's Laptop

↳ Julie copy/pasted from `Employee Q4 Bonuses` to Google Sheets

↳ Ryan exported `Employee_Q4_bonuses.xlsx` to Ryan's Laptop

↳ ⚠ Blocked Attempt Ryan uploaded `Employee_Q4_bonuses.xlsx` to Dropbox (personal)

Reduce risky user behavior

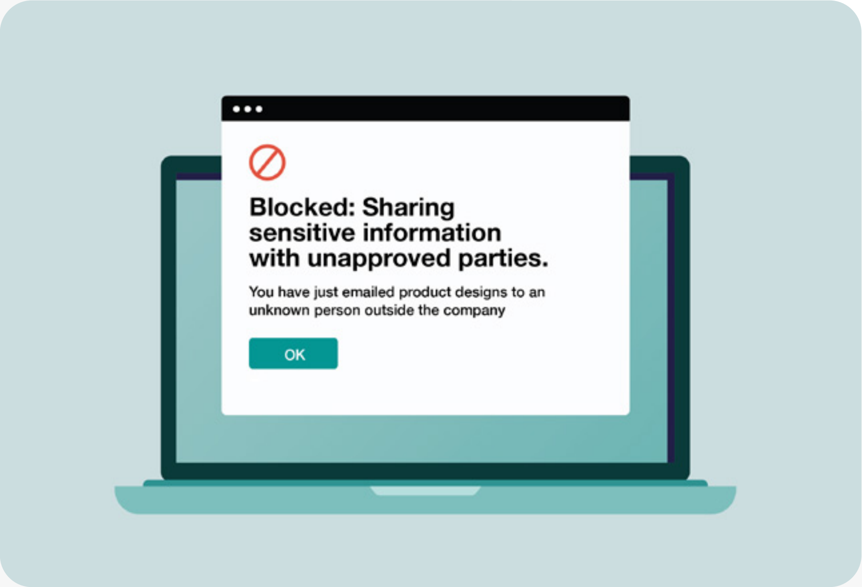
10

Educate employees on the proper handling of data in real time

Most risk-reduction strategies involve periodically training employees through video courses and following up on incidents with more training, which is often ineffective at changing user behavior. DDR can supplement these approaches with in-context education at the exact moment when an employee violates a policy which is proven to reduce common mistakes and mishandling of data by 80%.

Functional Requirements

- ✓ Accurate detection of risky behavior involving sensitive data
- ✓ Ability to block risky behavior in real time
- ✓ Customizable coaching messages based on the policy violation



Blocked: Sharing sensitive information with unapproved parties.

You have just emailed product designs to an unknown person outside the company

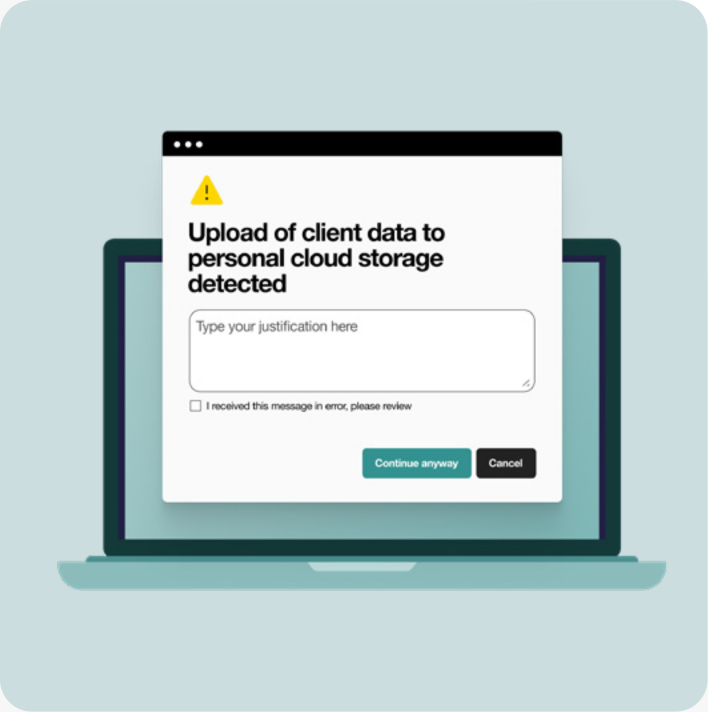
11

Allow employees to override blocking for justified business use cases

Some products take an all-or-nothing approach to data security, either simply flagging risky behavior for later investigation or blocking things in a way that stops business until someone contacts IT for an exception. DDR offers a middle approach that can protect data but also provide flexibility when there are approved business exceptions – such as uploading client data to a cloud storage service that otherwise wouldn't be allowed but in this case it's requested by the client. Employees can be warned of the risk of their intended action but can continue the process by providing a justification.

Functional Requirements

- ✓ Accurate detection of risky behavior involving sensitive data
- ✓ Ability to pause and resume potential risky behavior in real time
- ✓ Configurable option to allow override for policy violations based on risk level



Upload of client data to personal cloud storage detected

Type your justification here

□ I received this message in error, please review

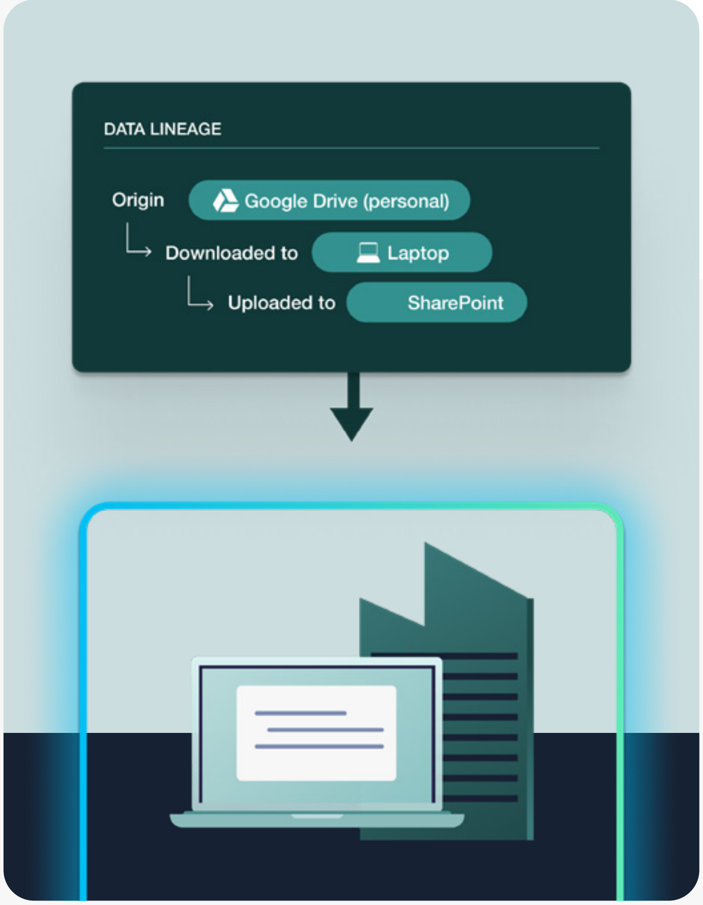
12

Risky data infiltration by new employees

New employees can bring confidential and protected data with them from their previous employer. This is a different kind of insider risk and can represent a huge liability for your business. DDR traces the lineage of all data, allowing you to detect potentially sensitive material entering your environment.

Functional Requirements

- ✓ History of all data movement within the company, including data originating from external sources
- ✓ Ability to query historical events for ingress of sensitive data in a specific time frame, such as when an employee first starts



DATA LINEAGE

Origin Google Drive (personal)
Downloaded to Laptop
Uploaded to SharePoint

Perform internal investigations

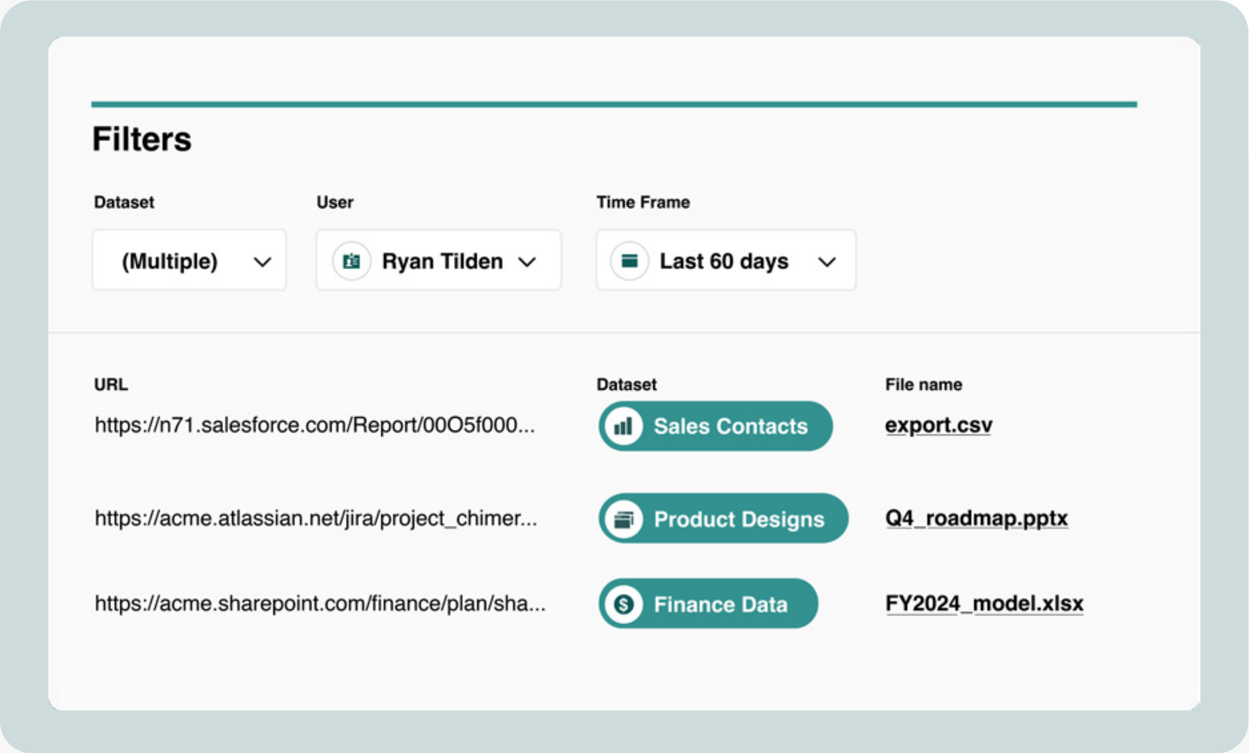
13

Capture a record of all employee activity for all data to support investigations

It is a common practice to start an investigation into employee activity following a trigger event, such as when an employee leaves for a competitor. DDR supports these workflows by capturing and visualizing all the data an employee interacted with during their entire tenure at the company.

Functional Requirements

- ✓ Tracking of all interactions with data, including opens, uploads, shares, etc.
- ✓ Ability to query events for specific users, specific types of data, and specific time periods of interest



Filters

Dataset: (Multiple)

User: Ryan Tilden

Time Frame: Last 60 days

URL	Dataset	File name
https://n71.salesforce.com/Report/00O5f000...	Sales Contacts	export.csv
https://acme.atlassian.net/jira/project_chimer...	Product Designs	Q4_roadmap.pptx
https://acme.sharepoint.com/finance/plan/sha...	Finance Data	FY2024_model.xlsx

14

Capture activity on devices without physical access to the device

Imaging a device using forensic software can provide many details regarding employee behavior useful in an internal investigation, but it usually requires access to the device. DDR captures many of the same events automatically and continuously, storing it securely in the cloud. This makes it possible to conduct investigations in cases where it would be inconvenient or impossible to image a device, such as when an employee does not return a company laptop or the laptop has been destroyed.

Functional Requirements

- ✓ Track events on devices and store associated metadata in the cloud
- ✓ Ability to query and view events such as web app usage, cloud app usage, AirDrop usage, and more

Action: Compress File

Previous file path: D:\Users\chris\client_list-q4.xlsx

File size: 7.97kb

md5 hash: 0c5c0eb72111f738b863828273c7263

New file path: D:\Users\chris\2023_GTM.zip

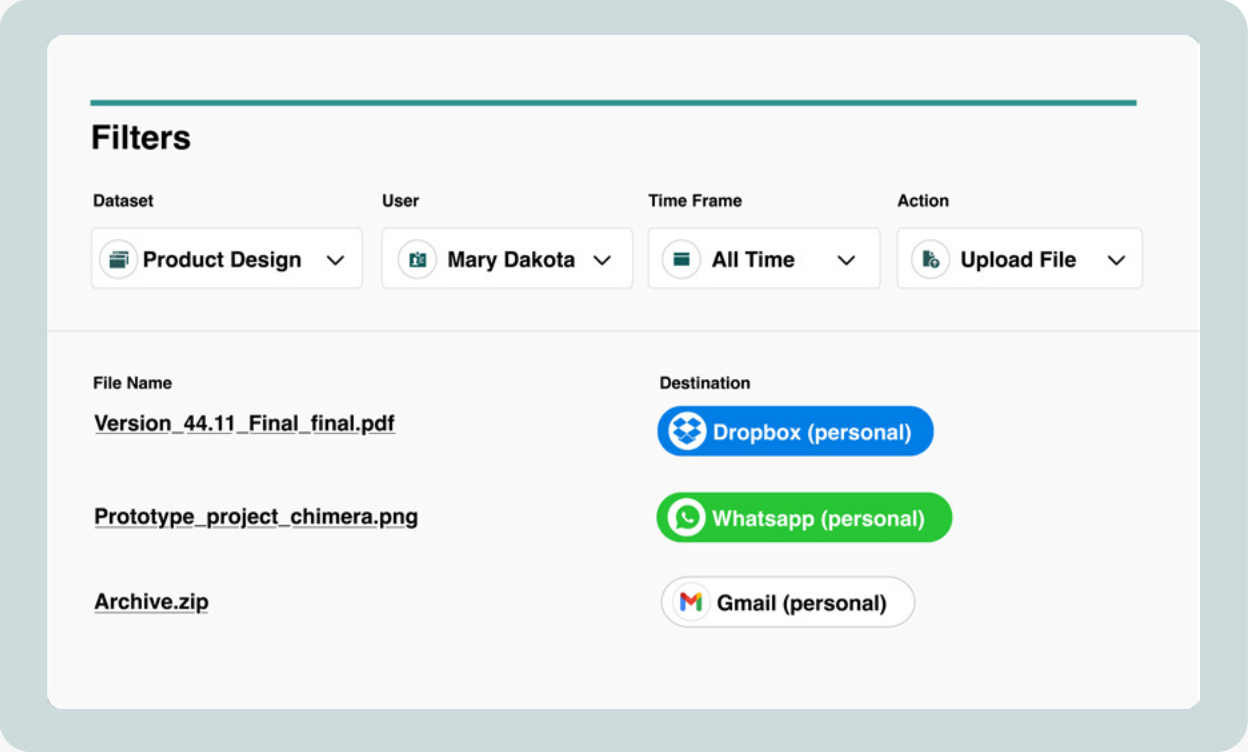
15

List all data employees have in their personal possession

When an employee or contractor leaves the company, DDR can provide a record of all company data they took copies of. Any severance agreement can require the return or destruction of company data in an employee's possession.

Functional Requirements

- ✓ Tracking of all operations with data, including opens, uploads, shares etc. and any personal or uncontrolled data destinations
- ✓ Query the full history of an employee's actions and list any data they removed from the company



Filters

Dataset	User	Time Frame	Action
Product Design	Mary Dakota	All Time	Upload File

File Name	Destination
Version_44.11_Final_final.pdf	Dropbox (personal)
Prototype_project_chimera.png	Whatsapp (personal)
Archive.zip	Gmail (personal)

About Us

Cyberhaven is the data security company revolutionizing how companies protect their most important information from theft and misuse. Until now, security products only recognized and protected a limited range of data types because they relied on finding patterns in the content itself. Our data tracing technology analyzes billions of events surrounding every piece of data to better understand and classify it, allowing for protection of a much broader range of sensitive data in any form, anywhere it goes.

To learn more about Cyberhaven, visit cyberhaven.com or email us at sales@cyberhaven.com