8.2.4 Canopy Software

Canopy's Data Breach Response Software

When a cybersecurity event occurs, incident response teams must race the clock to determine whether it is legally considered a breach. Was personally identifiable information (PII) or protected health information (PHI) compromised? If so, they could be bound by strict, non-negotiable notification deadlines enforced by GDPR, HIPAA, FERPA, and other data privacy regulations — or risk consequences like fines and damage to their reputation.

Canopy's patented Data Breach Response software applies AI and machine learning to:

Data Mining: Canopy's hundreds of machine learning algorithms are continuously trained to detect PII/PHI in any data set, from emails and text documents to spreadsheets, PDFs, and many other file types. Whether data is structured or unstructured, the software immediately scans it, unpacks and categorizes the files, and classifies the PII — no prior data normalization necessary. Canopy often completes processing within hours, then generates an automatic **Impact Assessment Report** that provides an overview of the data set, including the types and quantities of detected PII elements and how many documents contain them.

This AI-powered data mining is much faster than traditional approaches like iterative keyword searches or regular expressions (regex), so a single person can typically estimate the project scope and review cost on the same day they begin their assessment. Canopy is also significantly more accurate, narrowing reviewers' focus to the sensitive documents so they don't waste time & money needlessly reviewing documents that don't contain PII/PHI. (Case Study: Morae Saves Client Over $200,000 on Data Breach Response)

PII Review: Canopy's Data Breach Response software helps teams work significantly faster through PII Review while simultaneously decreasing the risk of human & keystroke error. It uses machine learning to make it both fast and easy for reviewers to link the PII/PHI detected in data to people. PII is clearly highlighted as reviewers click through documents, enabling them to quickly create entity profiles for individuals and connect them to breached data elements — all while maintaining links back to source documents. As Canopy learns about a specific project, its AI turns the process of linking PII to entities into a simple "accept or reject" workflow, eliminating both the need to copy-and-paste data into spreadsheets and the risk of error associated with this manual process. (Case Study: Wotton + Kearney Speeds Up Data Breach PII Review by 15%)

Entity Resolution: The end goal of any data breach response project is a consolidated list of who was affected, including their compromised PII, for notification. Canopy's Data Breach Response software features advanced entity management functionality that takes the heavy lifting out of this traditionally challenging process.

In addition to automatically deduplicating identical people within an entity list, Canopy also suggests merging entities when one individual is referred to in varying ways throughout the data, as might be seen with nicknames, abbreviated names, or maiden names. This entity management functionality saves response teams significant time by removing the need to manually locate and match repeated references to the same

person across spreadsheets or via custom SQL databases. (Case Study: Canopy Achieves “Impossible” Data Breach Response for Hospital Network)

Canopy’s Privacy Audit Software

In today’s digital world where organizations process more personally identifiable information (PII) and protected health information (PHI) than ever before, one can do everything right and still experience a cyber incident. Privacy Audit makes Canopy’s leading AI-powered PII detection available for proactive use at the enterprise level. The software zeroes in on PII, delivers a complete picture of how organizations process data, and provides critical insights to help mitigate risk *before* a breach occurs.

Enterprises can use Privacy Audit as part of a robust privacy program to:

Analyze: Privacy Audit is powered by hundreds of advanced machine learning algorithms that zero in on and classify the PII in an email inbox, file share, or any other data set, from driver’s license and social security numbers to financial data, medical information, and much more. Within a few hours, organizations get an Impact Assessment Report with a high-level analysis of what types of PII (and how much of it) the software detected in their data, and they can dive deep by clicking through individual documents to assess the context surrounding PII disclosure. Privacy Audit sorts documents by the amount of PII they contain to easily focus on the most sensitive and risk-prone files. It also offers filtering to view all documents containing a specific type of PII (like social security numbers) with one click.

Evaluate: Traditionally, singular cybersecurity policies and training have been implemented across an entire organization. But departments like Human Resources, Finance, Legal, and Sales handle different types of data in significantly different ways, and their cyber training and policies should account for that.

With metrics from Privacy Audit, organizations can compare sample data sets from one department or a group of similar people and note how they handle sensitive information. They can then use these insights to help form or improve privacy programs, enabling employees to work productively with a minimized risk of compromising PII.

Evolve: Cyber threats are constantly evolving and we’re continuously discovering new ways to work securely, so privacy programs must be adaptable. Organizations can revisit data over time with Privacy Audit to check that privacy programs are resonating with employees. Privacy Audit also provides the data needed to have informed conversations about policies and identify opportunities for improvement. By allowing both high-level and granular visibility into how employees are handling sensitive data, Privacy Audit makes it possible for enterprises to track compliance, detect gaps, and effectively mitigate risk before an incident occurs.

Case Study: How Intevac Is Using Privacy Audit to Protect Employee Data

Owned/Supplied by :	**Canopy Software**
Used by :	**Canopy Software**