Canopy

CASE STUDY

How Intevac Is Using Privacy Audit to Protect Employee Data

THE COMPANY

Intevac is a leading maker of thin-film equipment and photonics technology, providing solutions for the technology and vacuum coating industries as well as digital vision sensors and systems for the defense industry. They are headquartered in Santa Clara, California, with additional offices throughout Asia.

THE CHALLENGE

Amid an increasingly volatile threat landscape, Intevac's IT team launched a comprehensive privacy initiative to ensure that they were appropriately handling sensitive employee data. They needed a robust data mining tool to analyze their repositories and detect personally identifiable information (PII).

THE SOLUTION

After months of searching for the right software, Intevac selected Canopy's Privacy Audit. The IT team quickly completed implementation, training, and onboarding, then began analyzing one department's PSTs. They had their first Impact Assessment Report within hours.

THE RESULT

Privacy Audit uncovered thousands of unique PII elements, including high-risk data, in a matter of hours. Intevac's IT team was able to see the context surrounding PII disclosure on a per-document basis as well as generate high-level reports for leadership. This gives Intevac the insights necessary to customize its data governance policies and cybersecurity training.

canopyco.io | contact@canopyco.io

v20211008

Canopy

A Holistic Look at Protected Data Processing

Consumers are sharing more personal data than ever before, and the occurrence and severity of data breaches is on the rise. Corporations have an ethical obligation to protect customers' personally identifiable information (PII). They have growing regulatory responsibilities, too, like those mandated by the California Consumer Privacy Act (CCPA) in Intevac's home state.

These obligations extend beyond customer data. Organizations like Intevac, with 250+ employees globally, must also safeguard the sensitive data of employees. Intevac's IT team needed to gauge the company's level of risk should an incident occur.

In early 2021, they launched a comprehensive initiative to better understand how Intevac was storing and handling employee PII.

A Simple Solution for a Complicated Problem

Kicking off their privacy initiative, Intevac's IT team had four primary goals:

1. Identify the PII on their network,
2. Understand how it was stored,
3. Know how employees were sharing it, and
4. Uncover how it was being accessed.

They began researching software solutions that would allow their team to easily and accurately data mine for PII in massive data sets, but encountered two recurring problems:

1. Few solutions provided the level of essential detail — Intevac needed a streamlined workflow that would not require looking at a high rate of false positives.
2. The software options that came close to meeting their needs required installation, often behind Intevac's firewall and security protections, requiring much more effort than the team was able to dedicate.

"We have some security apps that we've been working on installing for literally years because they're so complex," said Intevac's IT Director Brenda Thrasher. "Even training on them is difficult, and they're super expensive, too. We needed a software solution that would get us up and running as quickly as possible."

> "We needed a software solution that would get us up and running as quickly as possible."
>
> **Brenda Thrasher**
> IT Director | INTEVAC

Brenda and Scott Menhennet, IT Management at Intevac, searched for six months before turning to their security partner for a recommendation. That's how they found Canopy's Privacy Audit software, and its advanced AI-powered PII detection and classification seemed to be exactly what they needed.

Putting the Power of AI to Work

Intevac used Privacy Audit to analyze a sample set of their own data. After less than a full day of training with Canopy's Customer Success team, Intevac's Information Security Analyst Eric Piazza was up and running quickly — no software installation required.

"Canopy made the training and onboarding process really simple," Eric said. "I didn't need to install anything to get started. The standard Privacy Audit template for analyzing data is out-of-the-box, and it was a breeze to use in the real world."

Canopy

After training, Eric uploaded the initial data to Canopy's secure application. Privacy Audit analyzed the 10 GB PST in just over three hours, its advanced machine learning algorithms honing in on and classifying all detectable PII elements. It then generated an Impact Assessment Report that summarized the PII found within the PST's more than 100,000 emails and documents.

Eric expected to find some low-risk personal information — like employees' names or dates of birth — but once he dug into the data, he was surprised by the results: Privacy Audit detected thousands of unique PII elements. In addition to viewing the high-level Impact Assessment Report, Eric was able to click through the documents themselves and see the context surrounding how employees were sharing sensitive data. Privacy Audit highlighted each PII element for fast and easy review, and showed the total amount of PII detected in each file to help guide Eric's focus to the most sensitive documents. To confirm the trend, Eric uploaded another PST from the same department and discovered similar findings.

"The amount of personal information that Privacy Audit found in our data was surprising," said Eric. "Just in one person's inbox, there were massive spreadsheets with high-risk PII, and we had no idea. I could quickly tell which documents were important by looking at PII density, and could even click through individual emails to see what PII they contained, who sent it, who it was sent to, where each file came from — it's very thorough."

Visual Reporting Exposes Risk and Makes Mitigation Easy

After exploring the software and analyzing the data, Eric shared the reports from both PSTs with Brenda and Scott, who were easily able to evaluate the findings thanks to Privacy Audit's transparent and user-friendly reporting.

"Privacy Audit told us right up front what we were dealing with," said Scott. "Canopy's Impact Assessment Report dashboard cleanly displayed the number of PII elements and sensitive documents it found, categorized by type, so that we didn't have to decode one big data dump. The reports are exactly what we need to show our executive team."

Unparalleled Processing Power and Speed

10 GB
the initial PST that Intevac uploaded

110,000+
emails and documents contained in the PST

3.5 hours
for Canopy to generate a report of PII findings

Canopy

Privacy Audit's speed paired with its automatic reports make it an ideal tool for a lean team like Intevac's to accurately analyze PSTs and other data sets from across the company quickly and easily.

"Canopy's Privacy Audit gives us the results we need much faster than other tools," said Eric. "Every company across the board should be doing this to protect their employees, and their business."

> "Using Privacy Audit's insights and reporting, our team can sit down with each department to show them how they're actually handling PII, explain the potential consequences of those actions, and develop a safer way forward."
>
> **Scott Menhennet**
> IT Management | INTEVAC

Intevac & Privacy Audit: A More Secure Future

Intevac's IT department is blazing a trail by working proactively to better safeguard employee PII. It starts with continuing to assess and understand how data is currently handled at Intevac with the help of Privacy Audit.

The key questions that Intevac and other companies pursuing a data-driven approach to security improvements and risk reduction must answer include:

- Can data be shared in a more secure way?
- Can it be deleted when it is no longer useful?
- Are employees following our policies for handling sensitive data?
- Is there PII hidden in surprising places?
- What is our overall risk profile?
- How can we identify mitigation strategies proactively?

The team also understands that there probably isn't a one-size-fits-all approach that will work for the entire company. Each department has its own unique needs and workflows, and broad data privacy education will be ineffective on its own. So Intevac is taking a novel approach by:

Analyzing the data of one group or department,

Evaluating that group's specific needs with leadership, and

Evolving their cybersecurity training program and data handling policy to speak directly to that group's daily functions.

"We know that cybersecurity training can be lengthy, and it often doesn't address trainees' specific workflows," said Scott. "Using Privacy Audit's insights and reporting, our team can sit down with each department to show them how they're actually handling PII, explain the potential consequences of those actions, and develop a safer way forward. This customized approach will be much more effective than generic training."

The goal is to provide a training experience that is more engaging for employees, and therefore will lead to actual change across the company.

Canopy

Once these policies and training are in place, Intevac's IT team can transition to using Privacy Audit as its name suggests — to audit that departments are adhering to safe data practices, thereby mitigating risk in the event of a breach.

In Brenda's words: "The bottom line is simple: Protecting the PII that we're responsible for — including that of our employees — is a core part of our privacy program. Canopy's Privacy Audit gives us a critical capability in this regard."

> "The bottom line is simple: Protecting the PII that we're responsible for is a core part of our privacy program. Canopy's Privacy Audit gives us a critical capability in this regard."
>
> **Brenda Thrasher**
> IT Director | INTEVAC

Ready to Gain More Insight Into Your Data?

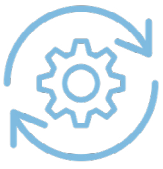
Email our team of Foresters at contact@canopyco.io to request a demo of Privacy Audit and see how it can enhance your privacy program by enabling you to:

Analyze

Privacy Audit is powered by hundreds of advanced machine learning algorithms that hone in on and classify the PII in an email inbox, a fileshare, or any other data set, from driver's license and social security numbers to financial data, medical information, and much more. Dive deep by clicking through individual documents to assess the context surrounding PII disclosure, or view a high-level analysis with Privacy Audit's reporting.

Evaluate

Departments like HR, Finance, Legal, and Sales handle data in significantly different ways, and their cyber training and policies should account for that. With metrics from Privacy Audit, you can compare sample data sets from a group of similar employees and note how they handle sensitive information. Use these insights to help form or improve your privacy program and minimize the 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. Revisiting your data over time with Privacy Audit helps you check that your privacy program is resonating with employees. It also provides the data needed to have informed conversations about your policies and identify opportunities for improvement.