GROUND LABS

CASE STUDY

PCI and PII Data Discovery Achieved:
Leading Utility Provider

THE CHALLENGE

A utility provider managing data for hundreds of thousands of residents

In early 2021, a water and sewage utility provider suffered a data breach. The company provides drinking water in Australia as well as collects and treats sewage. As a government-owned entity servicing a region of over 500,000 people, the utility company is responsible for a large volume of personally identifiable information (PII) and payment card industry (PCI) data, including credit card numbers.

After suffering a data breach in early 2021 — both a major issue for the customers and a reputational problem for the brand — the utility company began searching for a solution to help it identify where its customers' PII and PCI data was being stored.

THE JOURNEY

The search for a PCI compliance solution

The airline was storing cardholder data across a variety of servers, databases, and other locations, including O365, OneDrive, Notes, Teams, Forms, Azure, SharePoint online, Hadoop HortonWorks & Cloudera, and AWS Glacier. With millions of customers, the company needed urgent help achieving Payment Card Industry (PCI) compliance. PCI compliance is critical for businesses handling credit card numbers due to the heightened number of data breaches, to protect customers from credit card fraud.

Payment card fraud losses reached **$28.65 billion worldwide** in 2019, according to a Nilson Report.

Hackers are highly motivated to steal credit card data. If they gain access to sensitive data including primary account numbers, cardholder names, and authentication codes, hackers can impersonate the cardholder, use the card to make purchases, and even steal the cardholder's identity.

In addition, if a data breach occurs again and hackers gain access to additional customer PII, this utility provider could suffer further financial and reputational burdens. Customers lose trust in businesses after data breaches, and the costs of this add up.

To protect sensitive data and maintain customer trust, the utility provider needed a solution to help it accurately, quickly and easily identify where PII and PCI data was stored, enabling the company to remediate and protect the sensitive data before any future compromise. The company turned to Ground Labs for help scanning and identifying PII and PCI data across its network.

THE SOLUTION

Ground Labs' Enterprise Recon helps utility companies discover sensitive data

Because this utility provider handles such a high volume of credit card numbers and other personal information from customers, the team knew it had a monumental task ahead to find where all that data was being stored. It decided to partner with Ground Labs and now relies on Ground Labs' award-winning Enterprise Recon software to maintain ongoing awareness of where sensitive data is stored.

The company uses Enterprise Recon PII and Enterprise Recon PCI to find where credit card numbers and PII are stored within both structured and unstructured data sources, including files, databases, emails, cloud, big data, and more. After scanning, Enterprise Recon PII allows the team to view and analyze where sensitive data resides and immediately contact the owners to take action.

Ultimately, Enterprise Recon PII provides a blueprint of the PII and credit card number storage locations across the organization, allowing the company to ensure on an ongoing basis that it is not storing any sensitive data unnecessarily, and when necessary, that the company is storing them securely to protect consumer information.

THE RESULTS

Enterprise Recon identifies 60 million credit card numbers in the airline's ecosystem

After beginning the scanning process with Ground Labs' Enterprise Recon, the utility provider identified millions of instances of customer credit card and PII information. In spite of the large volume of improperly stored sensitive data, Enterprise Recon's delegated remediation feature allowed the company to assign different teams to address the risk through Enterprise Recon so this massive undertaking didn't fall solely on the shoulders of IT.

To learn more about how **Enterprise Recon** can enable your business to become PCI compliant, click **here**.

GROUND LABS

[1] "Cost of a Data Breach Report," IBM, 2019, https://www.ibm.com/downloads/cas/ZBZLY7KL.