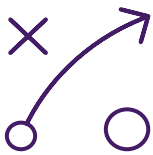


PCI Compliance Achieved: Leading Gaming & Hospitality Company



THE CHALLENGE

A hotel and casino managing payments for millions of customers

A major leader in gaming and hospitality operating more than 50 properties across the United States and the Middle East was quickly growing into new locations. With so many different hotel and casino locations, the company manages a high volume of credit card data and other personally identifiable information (PII) from countless customers.

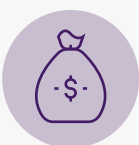
The company needed to protect against data breaches and ensure it was meeting payment card industry (PCI) compliance requirements, as well as other national and local compliance standards. Companies operating in the gaming industry have to jump through countless regulatory hoops, ensuring compliance with thousands of local, state, and federal regulations that sometimes contradict each other. Many companies approach this by choosing the strictest law they need to comply with, and that tends to cover the rest.



THE JOURNEY

The search for a PCI compliance solution

The gaming and hospitality company was storing cardholder data across file shares, emails, and some desktops. With so many customers, the company needed urgent help achieving Payment Card Industry (PCI DSS) compliance. PCI compliance is critical for businesses handling credit card numbers to protect their customers from fraud, especially with the heightened number of data breaches.



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.

If a data breach occurs and hackers gain access to additional customer PII and credit card data, this gaming and hospitality company could suffer significant financial and reputational burdens. Customers lose trust in businesses after data breaches, and the costs of this add up.



An IBM report found that the **average cost of lost business due to a data breach in 2019 was \$1.42 million.**¹

To protect sensitive data and maintain customer trust, the gaming and entertainment company needed a solution to help it accurately, quickly and easily identify where credit card data and other PII 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 cardholder data across its network, with a goal of becoming PCI compliant and also maintaining compliance with a variety of other privacy regulations.

After achieving ongoing PCI compliance, the company expanded its data discovery search to include PII, including social security numbers, passport numbers, and addresses to maintain CCPA, CCPR, GDPR and SOX compliance.



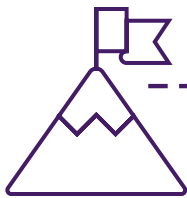
THE SOLUTION

Ground Labs' Enterprise Recon helps the gaming and hospitality company maintain privacy law compliance

Because this company handles such a high volume of credit card numbers and PII, 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 meet and maintain compliance with PCI and other privacy regulations.

The company uses Enterprise Recon PRO to find where credit card numbers are stored within both structured and unstructured data sources, including files, databases, emails, cloud, big data, and more. After scanning for credit card numbers and other data types, Enterprise Recon allows the team to view and analyze where sensitive data resides and immediately contact the owners to take action. Before implementing Ground Labs' solution, approximately 3-6 people were fired weekly at the company as a result of improperly handling sensitive data, and Enterprise Recon has helped improve sensitive data storage across the board.

Ultimately, Enterprise Recon provides a blueprint of the credit card number and other PII storage locations across the organization, allowing the gaming and hospitality company to ensure on an ongoing basis that it is not storing any addresses or credit card, social security, or passport numbers unnecessarily, and when necessary, that the company is storing them securely to protect sensitive 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 gaming and hospitality company identified millions of customer credit card numbers and other PII that were being stored in the wrong places. Enterprise Recon's delegated remediation feature enabled the company to assign multiple teams to address the risk using 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.](#)

