CASE STUDY

CARA Meets PCI Requirements and Gains Network Visibility with LogRhythm

Project Management Officer: LogRhythm gives us a comfort level that we are meeting the PCI requirements across our vast network of restaurants CARA at a glance.

Customer

CARA
Vaughan, Ontario, Canada

The Challenge

- CARA needed to implement a log management and monitoring solution that would greatly simplify the PCI compliance and audit processes.
- CARA's cardholder data environment spans 700+ restaurant locations across Canada.
- More than 500 franchisees depend on CARA for a PCI compliant payment processing environment.

The LogRhythm Solution

- LogRhythm's out-of-the-box PCI features yielded immediate actionable reports for CARA.
- LogRhythm distills tens of millions of data points down to relevant alerts to improve the network's security posture.

The Results

- CARA can now confidently offer a fully managed and PCI compliant POS environment to its franchisees.
- CARA has a better picture of what's happening at each location and can respond promptly—often even before the franchisee is aware there is a problem.

Future Plans

- CARA is looking into pulling logs from systems that are not part of the PCI scope: telephone systems, HVAC, refrigeration units.
- CARA plans to expand operational visibility to make overall business operations more efficient.

Introduction

CARA is a privately held company that recently celebrated its 125th anniversary. CARA owns many of Canada's favorite restaurant brands including Swiss Chalet Rotisserie & Grill, Harvey's, Kelsey's, Montana's, and Milestones Grill & Bar. Though all these brands are distinct, they are tied together by one single purpose, and that is to provide the perfect guest experience, every time.

There are more than 700 restaurants in the CARA network all across Canada. About 100 restaurants are corporate owned and the rest are franchised. CARA extends that concept of the "perfect experience" to its franchisees. Rik Steven, a manager in the corporate project management office, explains what this means. "When someone buys a restaurant, the company helps build the building and gets the franchisee all set up to serve its guests. That total experience includes the computer networking, the point-of-sale (POS) systems, and payment processing. Everything is completely managed by CARA Operations," says Steven.

When customers pay their bill with credit cards, the payments are routed through an private link back to CARA's data center. All processing goes through that data link, so in effect CARA is a payment service provider to its franchisees. This makes the company a Level 1 merchant with very high requirements for PCI compliance. Says Steven, "Not only is CARA responsible for its own compliance, but the company is ultimately responsible for delivering compliance to its franchisees."

When it comes to credit card processing, there are two areas in which the company accepts payment cards. One is in the restaurants where the POS system includes a wireless version for full service restaurants and a wired version for the quick service restaurants. CARA also has an application that supports card acceptance over the phone or via the Internet for take-out and delivery orders for the Swiss Chalet locations.

The Business Challenge

The PCI Data Security Standard (DSS) dictates the requirement for logging and monitoring of all systems involved in the collection, transmission, processing and storage of highly sensitive cardholder data. As a service provider to more than 700 restaurants, CARA Operations needed to implement a solution that could log and monitor all PCI-related activity in all the locations and across all environments (i.e., in-store, phone in and Web-based). The sheer magnitude of this project was daunting.

Because PCI compliance adds little value to a company's bottom line, a pressing concern was to implement a cost effective log management solution that could not only automate and streamline the compliance process but also deliver operational benefits as well. For example, securing the network that spans all restaurant locations is CARA's responsibility. Steven says the company wanted an enterprise log management system that could provide security alerts and deliver insight to what is happening at individual locations.

Why LogRhythm?

CARA evaluated several enterprise-level log management systems before selecting LogRhythm, and LogRhythm's product delivered several unique solutions to CARA's needs.

First , the architecture of the LogRhythm solution easily supports CARA's extensive network of locations. The logs from all the restaurants are funneled over the private connections to two different data centers for redundancy, and then into one appliance for the recording. A total of three appliances meet the logging needs for the entire enterprise.

Next, LogRhythm's out-of-the-box pre-configuration for PCI compliance meant that CARA saved money and resources by not having to hire a cadre of security consultants for the implementation. "With the other solutions, we were concerned we'd need a security team to get it installed and set up. We were afraid of the learning curve," explains Steven. "We invited LogRhythm to do a proof-of-concept for us. We found it fascinating that they could have it up and running so quickly. LogRhythm worked right off the bat," according to Steven. In fact, in the proof of concept, LogRhythm discovered problems on CARA's network that day. "We found it impressive that we immediately had an actionable report that first day," says Steven.

Third, LogRhythm's PCI compliance tools helped CARA get up to speed quickly and easily. "There's so much to PCI, so when we found ourselves having to achieve compliance, there were so many gaps that had to be addressed," Steven says. "We love the fact that this one tool addressed so many of the requirements, that it was so easy to put into place, and that we could use it immediately. It was much simpler than most of the other tools we looked at—certainly as compared to other tools and components we had to implement for PCI. For instance, when we brought in the application firewall and entertained the idea of an intrusion prevention system and the effort to get those configured and working and in place compared to LogRhythm, LogRhythm was a breeze."

Implementation and Operation

Once the decision was made, LogRhythm engineers helped CARA through the entire implementation process. The company collects logs pertaining to payments from every restaurant, regardless of whether it is a franchise store or corporate-owned. CARA pulls logs from each location's primary POS server, numerous local POS terminals, and network switches and routers. This amounts to tens of millions of data points a day.

"The amount of information that comes back to us was just overwhelming to begin with because PCI requires us to be monitoring that all of the time," according to Steven. "The LogRhythm tool is great because it boils down to what you need to see as opposed to all of that information coming in. It shows us relevant alerts, so being able to not have to deal with all of the information but just the alerts that come up is much easier for us to manage."

From a PCI perspective, the alerts let the CARA security administrators know if there are multiple attempts to gain access to a server, or if someone enters a bad password. "There are numerous things we can see," says Steven. "For instance, we want to be aware of system shut downs, but especially we want to know about attempts to connect to the server that shouldn't be occurring except for administrative staff or service desk staff. No one should be accessing the POS servers so we want to be aware of that happening at any time."

When CARA first rolled out the logging solution, the company didn't have enough people on staff to monitor it every day, so they engaged the services of a managed service provider. This company provides monitoring for the LogRhythm console as well as a few other management tools. "They have an operating center that is always watching those tools for us so when the alerts do come, if they are important alerts or something we need to be made aware of right away, they contact our service desk and let them know," explains Steven. "That means we don't have to have somebody in our office looking at the tool the whole time." However, CARA is transitioning from this service to an in-house security professional now that the system is fine-tuned and he has a good comfort level with how it works.

"Our in-house resource regularly pulls out reports or summaries for management at the end of the month or the quarter," says Steven. "These reports give us an idea of what types of activities are being picked up by this tool. We post

these reports to a shared folder so they can be accessed and reviewed by management. The insight we get is very helpful."

The Results

Steven says CARA began reaping the benefits of the LogRhythm system right away—literally as soon as they plugged it in. "We had actionable reports from the very first day," says Steven. "Since we've implemented the LogRhythm system, we have an awareness of the stores that we didn't have before. We can see when something unusual is happening. It's very useful to have somebody connect and monitor what's going on."

In terms of PCI compliance, LogRhythm has helped CARA meet requirements that the company otherwise wouldn't have been able to meet. "The PCI QSA comes into our audit and sits down with our administrator. He goes through the LogRhythm reports and literally checks off everything in Section 10 that we've got everything in place, including file integrity monitoring," according to Steven.

He adds, "I would absolutely say we have gotten a good ROI on this product. We have that comfort level that we're monitoring these systems and meeting that PCI compliance for our franchisees. LogRhythm has enabled us to achieve PCI compliance two years in a row now since we've started on this path."

Future Plans

Steven says that CARA is looking to reap benefits beyond PCI compliance. Since LogRhythm can work with any kind of log data, the company is looking at collecting operational data from other IP-enabled equipment, including the telephone system, the restaurant refrigeration units and the heating/ventilation/air conditioning (HVAC) systems. "LogRhythm's so good at pulling logs back and helping us drill down to meaningful information," explains Steven. "There are other systems that aren't part of the PCI scope; for example, building and operational systems, the accounting system, the payroll system. We can pull data back and correlate it and use the same tool to analyze what's going on with these other applications and utilities. This should help us improve operations in ways that can yield a competitive advantage."

Steven says they also are building out their reporting capabilities in order to give company executives more visibility. "LogRhythm gives us information that eliminates gaps in our oversight of the business." With better visibility and real-time, actionable insight, it's easier to produce that "perfect guest experience" for everyone involved.