



## Case Study

### *Gordon Food Service Turns to Q1 Labs for Threat Management & PCI DSS Compliance*



#### Background

Gordon Food Service® ([www.gfs.com](http://www.gfs.com)), founded in 1897, is North America's largest family-owned and managed broad line food service distributor that offers more than 16,000 GFS® and nationally-branded products to more than 45,000 customers in the United States and Canada. The company has operations in the U.S. that extend from Michigan to Florida, and across Canada from British Columbia to Newfoundland and Labrador. Gordon Food Service distributes a wide range of products – including beverages, dairy products, fresh produce, frozen foods, groceries, meats, poultry, seafood, and other supplies – to a broad market, including health care facilities, schools, and independent and chain restaurants. There are also 129 GFS Marketplace® retail stores that are open to the public that provide restaurant-quality food service products without requiring a membership fee.

#### Food Service and Network Security

Few observers probably view food service providers as being particularly technology

“QRadar had enough features and functionality – right out-of-the-box – to provide us with immediate value in the areas of compliance and security.”

#### Industry:

Food and Beverage; Retail

#### Key Benefits:

- ✓ Centralized network security management
- ✓ Easy-to-deploy and operate
- ✓ Significantly improved detection of network-based threats
- ✓ Outstanding customer service

focused, but Paul Gordon, the late and former Chairman of Gordon Food Service, was determined to take a decidedly different path by embracing the potential efficiencies that new technology might provide his business. For example, 20 years ago laptop computers were typically reserved for only the most senior sales executives in many companies, but Gordon saw the competitive advantages technology could deliver and outfitted *all* Gordon Food Service sales reps with the devices so they could stay on top of their client interactions and improve customer service and satisfaction.

With its network infrastructure as a competitive differentiator, Gordon Food Service takes security risks very seriously. As such, the

company recognized the need for visibility across its entire network, so any threat could be minimized and dealt with swiftly, without impacting the company's ability to meet customer needs and timelines. Ron Porritt, information security engineer for Gordon Food Service, found the company could not investigate questionable events that would show up in the organization's firewall logs. Most disconcerting was the inability to obtain additional information related to an event. Gordon Food Service technicians had no way to gain enough understanding to determine whether or not an event was a significant risk. It was time for Gordon Food Service to implement better monitoring practices across its growing network.

Tasked with identifying the best solution to help them define and properly respond to risk, Gordon Food Service representatives determined that their number one goal was investigative in nature. The product they sought had to be able to provide details around events that would allow them to understand what happened and determine if action needed to be taken. A secondary goal was also included in the project: as much as possible in current product offerings, the chosen solution needed to evaluate and respond to risk.

### **First Look at QRadar: Network Flow Analysis**

After reading various product reviews, conducting technical discussions with many vendors, and receiving demonstrations from several of them, Gordon Food Service identified Q1 Labs' QRadar security information and event management (SIEM) solution as the "clear winner" in flow and event log management. The biggest competitive advantage Gordon Food Service saw in QRadar was its ability to capture information and analyze all traffic flows occurring within the Gordon Food Service network.

Concerned that competitive offerings only provided a limited ability to provide important context around an event, Porritt explained, "With most other products, the only time they keep information about traffic is if some rule or exception is triggered to identify it as a concern. If there wasn't a rule to capture what you needed, the critical information was essentially thrown away."

After thoroughly evaluating the needs of Gordon Food Service for a comprehensive network flow collection and analysis solution, Porritt and the

**"In my 30 years of working with network vendors, Q1 Labs' service is unmatched."**

company's network team determined QRadar was the product that was best suited to meet the firm's requirements. "With QRadar, we can take any network behavior and look back to get information about its relative importance to the company's overall security posture," he noted.

During the evaluation process, Gordon Food Service experienced several key features and benefits that helped solidify its decision to deploy QRadar. At the top of the list was the product's ability to capture information on the flows of data coming into the network. This was the number one criteria for evaluation, and Gordon Food Service's representatives were very pleased with what they saw. They were also impressed with QRadar's ability to understand events, rank the events by risk, and create alerts on high priority events.

The initial set up and implementation of QRadar was straightforward. In two days, Gordon Food Service had its first QRadar console and network flow collector in place, collecting data and providing value right out-of-the-box. Over the next few years, the company added seven more collectors to analyze flow data across other parts

of the network and at the same time started to collect events from firewalls, VPN concentrators, and access control devices. Throughout his time as a Q1 Labs' customer, Porritt underscored how impressed he is with the company's support program. "In my 30 years of working with network vendors, Q1 Labs' service is unmatched," he stated.

### **QRadar Deployed: Log Management and Correlation Added to Meet PCI**

Like virtually every organization that processes credit card transactions, Gordon Food Service also needed to make certain it was in compliance with the Payment Card Industry Data Security Standard (PCI DSS). The company quickly realized QRadars was going to be very helpful in providing its PCI team with the validation it needed to show that the firm was properly monitoring and responding to network events.

The initial installation was expanded with a new collector aimed specifically at PCI traffic. Feeds from CheckPoint firewalls and Cisco VPN concentrators, routers, and switches were enhanced in line with PCI requirements. Gordon Food Service met its compliance mandate and QRadars remains a central component in its continuing need to evolve with ever-changing PCI requirements.

Not only did QRadars help Gordon Food Service address the compliance mandate from a logging and monitoring standpoint, but it was also flexible enough to enhance broader network and security monitoring requirements.

### **Gordon Food Service Today**

QRadar has helped Gordon Food Service significantly improve its ability to monitor and respond to security events. Q1 Labs' offering has been key in achieving Gordon Food Service's security initiatives to capture, analyze,

and data mine application and security event information that traverses its network in order to better manage threats. Since deploying QRadars on its corporate infrastructure, Gordon Food Service has been able to identify and eradicate a variety of network threats, including malware and viruses, along with network misconfigurations.

A QRadars user for four years, Gordon Food Service remains satisfied with its choice. "If we didn't have QRadars to help analyze the mountains of application traffic coming into and out of our network, it would have been nearly impossible to identify the anomalies that the company viewed as threats," said Porritt. "Moreover, QRadars had enough features and functionality — right out-of-the-box — to provide us with immediate value in the areas of compliance and security."

The company was also impressed by the level of customer support provided by Q1 Labs. According to Porritt, "The service that we received and continue to receive from Q1 Labs remains unmatched by almost any technology vendor that I've ever dealt with. The company's representatives are great — they are extremely proactive with their training, going so far as to organize one-on-one WebEx training sessions. In addition, a big plus is our ability to tune QRadars to achieve customized results, while still maintaining a comprehensive overview and thorough analysis of network activity."

About Q1 Labs as a company, Porritt added, "The responsiveness and integrity of this organization are unequalled. In fact, we never have to go through multiple layers of operators to get someone live in post-sales support. Also, I can honestly say that we have never had an inkling of buyer's remorse with Q1 Labs."

**"The responsiveness and integrity of this organization are unequalled."**



**Corporate Headquarters:**

**Q1 Labs, Inc.**

890 Winter Street  
Suite 230  
Waltham, MA 02451 USA

**Telephone:** 781.250.5800  
**Fax:** 781.250.5880  
**Email:** [info@Q1Labs.com](mailto:info@Q1Labs.com)  
**Web:** [Q1Labs.com](http://Q1Labs.com)

**DS040809A**

**About Q1 Labs**

Q1 Labs is a global provider of high-value, cost-effective network security management products. The growing company's flagship offering, QRadar, integrates previously disparate functions – including log management, network behavior analytics, and security event management – into a total security intelligence solution. QRadar provides users with crucial visibility into what is occurring with their networks, data centers, and applications to better protect IT assets and meet regulatory requirements. Headquartered in Waltham, Mass., U.S.A., Q1 Labs' customers include healthcare providers, energy firms, retail organizations, utility companies, financial institutions, government agencies, and universities, among others.

Copyright © 2009 Q1 Labs, Inc. All rights reserved. Q1 Labs, the Q1 Labs Logo, Total Security Intelligence, and QRadar are trademarks or registered trademarks of Q1 Labs, Inc. All other company or product names mentioned may be trademarks, registered trademarks, or servicemarks of their respective holders. The specifications and information contained herein are subject to change without notice.