Carhartt Solves PCI Compliance Conundrum

SUMMARY

Conforming to Payment Card Industry Data Security Standard (PCI DSS) requirements reduces risk and protects organizational value, but implementing controls without adding complexity or becoming bogged down with the management of lengthy procedures can be a challenge. Non-compliance can be costly, with fines and loss of business a heavy price to pay.

To create a threat-detection system that could meet and exceed PCI DSS security regulations, the global apparel maker Carhartt combined the following iSecurity and absSuite products to create this three-step compliance solution that runs on Carhartt's 80+ IBM i LPARs.

1. iSecurity Syslog software transfers IBM i log file data from all LPARs into Carhartt's centralized IBM QRadar server, which is used for organization-wide security information event management (SIEM) processing, problem detection, analysis, and reporting.

2. iSecurity Anti-Virus product scans the Integrated File System (IFS) for virus detection and alerting on over 40 different Carhartt IBM i systems that are dedicated to Carhartt's eCommerce solution.

3. absMessage software monitors messages and IBM i resources to spot issues and automatically alert on-call responders when a problem occurs.

This three-pronged solution helps Carhartt meet and maintain PCI DSS compliance, protecting it from incurring non-compliance penalties, avoiding possible suspension of credit card processing capabilities if a major breach occurs, and helping Carhartt maintain its reputation as a secure credit card processor with its customers, business partners, and vendors.

Here's how Carhartt solved these IBM i PCI DSS issues by using Software Engineering of America (SEA) products to create a compliance environment.

PROBLEM

Maintaining compliance with PCI DSS regulations was an exercise in risk management for Carhartt. The first goal was to prove Carhartt knew what risks and damages were likely to occur, and to be able to detect potential breaches. Carhartt also needed to prove how it could reduce or mitigate the damage if events occur that could lead to increased risks. Carhartt took steps to enhance its capabilities to identify business risks, assess and measure risks, and to take corrective action to reduce or eliminate risks.

> "It was also important to take work off our operators and put it in the hands of people who would have to correct the problems when error messages occur."
>
> —Gary Adkins
>
> IBM i SYSTEM ADMINISTRATOR
> **CARHARTT**

SOLUTION

To incorporate, consolidate, and simplify PCI DSS compliance reporting and improve its threat detection capabilities, the IBM i systems staff at Carhartt decided on a multi-pronged approach. The first step was to add SIEM reporting of security log events on their IBM i enviornment. Next, they added virus-protection software capable of protecting the IFS directory structure. Finally, to address PCI DSS monitoring and notification requirements, Carhartt added IBM i message and resource monitoring software. Products from several vendors were considered. The optimal solutions were picked from the iSecurity software suite as well as SEA's absSuite . iSecurity Syslog, iSecurity Anti-Virus, and SEA's absMessage software were ultimately chosen and quickly implemented.

RESULTS

The initial implementation stage began in March 2017 with Syslog integration and Anti-Virus scanning, two key components for PCI DSS compliance. The second stage, involving the implementation of absMessage, an important contributor to security management, began two months later.

Carhartt's IBM i environment consists of more than 80 LPARs. IBM i Syslog installation began on the company's development box and was completed in less than two hours. The rollout continued from there. Nearly all of the configurations and settings were to be the same on all LPARs. Use of the built-in EXPORT and DISTRIBUTION capability of the products provided a quick and easy implementation process.

The team found the best implementation method was to push the software to three or four LPARs at a time, completing 15 to 20 installations a day.

SYSLOG INTEGRATION

iSecurity Syslog provided a simple integration with IBM QRadar, the SIEM analysis and reporting component in Carhartt's environment. A few glitches were encountered--a couple of systems were experiencing communication issues with the SIEM server—but Carhartt IBM iSeries System Administrator Gary Adkins described them as independent issues from the Syslog product that were easily worked out. "Once we had systems in place," Adkins said, "the software deployment went smoothly."

ANTI-VIRUS

The Anti-Virus implementation was completed on over 40 LPARs devoted to Carhartt's commerce systems. It was set up to complete daily scans of the IFS, the repository for PC-based files in an IBM i environment. These files, which can contain viruses that are not harmful to the IBM i environment, are accessible by any PC-based user connected to an IBM i. Without protection, PC users can become infected as well.

The Carhartt staff handled most of the deployment, with some remote help from the SEA experts.

MONITORING AND ALERTING

After the installation of Syslog and Anti-Virus was completed and the IT staff was comfortable using those products, the rollout of absMessage took place. The monitoring and alerting system was the final piece for PCI compliance.

"It was also important to take work off our operators and put it in the hands of people who would have to correct the problems when error messages occur," Adkins said. "We wanted to have one central location where all the critical messages from all the LPARs could be seen. The bouncing around finding multiple screens in multiple locations needed to be eliminated. It's much easier to take appropriate actions from a central location."

That central location, the reporting LPAR, is referred to by the IT staff as "The Concentrator." All the other IBM i LPARs send their critical messages to the Concentrator where they can be viewed and responded to in a single pane of glass.

"We login and bring up the message console either online or through an IBM i session," said Adkins. "Although the operations crew is set up to monitor the systems, it doesn't require constant babysitting. When critical messages arrive, emails are sent to individuals trained for quick response."

For the rollout of absMessage, the software was installed on The Concentrator and pushed to other systems from there.

CONCLUSION

Using this multi-pronged approach, Carhartt was able to implement solutions for their PCI DSS requirements to maintain a vulnerability management program (IFS virus scanning), to integrate IBM i information into their security log systems (syslog integration), and to monitor and respond to system events as they occur (message and resource monitoring).

About Carhartt, Inc.

Established in 1889, Carhartt is a global premium workwear brand with a rich heritage of developing rugged products for workers on and off the job. Headquartered in Dearborn, Michigan, with more than 4,600 associates worldwide, Carhartt is family-owned and managed by the descendants of the company's founder, Hamilton Carhartt. For more information, visit www.carhartt.com and follow @Carhartt on Twitter.

About Software Engineering of America (SEA)

Established in 1982, Software Engineering of America has built a global reputation as a leader in datacenter software solutions. SEA is one of the most successful companies in the datacenter software industry, with products used at thousands of installations worldwide. Over 10,000 data centers of all sizes and configurations are utilizing one or more of SEA's products, including 9 of the Fortune 10 as well as 85% of the Fortune 500 Companies.