QSoftware

OVERVIEW

Challenge
- Reduce the effort and cost of producing audit reports and conducting internal security reviews
- Identify unknown risks in the ERP system so they could improve security.

Q Software Solution
QCloud Audit-as-a-Service

ERP System
JD Edwards World

Benefits
- Five days effort producing audit reports reduced to the click of a button
- Quarterly audit cycle reduced from six weeks to one week
- Actionable insights into security weaknesses
- No in-house technical effort needed.

"The results are so easy to read. It's just been amazing!"

Better results for much less effort; CTB, Inc. breaks the cycle of stressful security audits

The Problem

As a Berkshire Hathaway company, CTB, Inc. is required to audit its JD Edwards World security quarterly to ensure that its 650 users have appropriate access. The company also has annual external audits.

"Preparing for our audits was a nightmare," says Jennifer Leatherman, Director of Business Systems. "It's a moving target, because they look at something different every time. So we were usually reactive, focusing on the findings of the last audit to make sure the same issues didn't come up again."

"I was always worried about the JDE security. It's difficult to know where the weaknesses are, so I decided to focus on Segregation of Duties." Jen worked with CTB's accounting group to identify the key SoD rules. "We defined a basic set of rules covering Purchase to Pay, Order to Cash and so on. We knew we were only covering the basics, but we didn't know what we didn't know, so we'd only improve it when something showed up in an audit."

Reviewing security was very time-consuming. "We tried to produce reports to identify SoD issues, but we ended up with many pages of information that was difficult to interpret. On top of that, the auditors said that we needed to move the responsibility for reviewing security to our business controllers, rather than having it done by the IT team, who'd set it up."

Although that made sense, it caused huge problems. The controllers didn't understand JDE security and found it difficult to work with the reports. Finance responsibilities always took precedence, so it usually took about six weeks to complete each quarterly audit. The auditors kept chasing Jen for notification that it was complete, so she felt she was always running behind.

The situation grew even worse when they upgraded from A7.3 to A9.3 and moved towards Role-based security. The transition proved to be very challenging, and it took them a lot of effort through 2017/18 to get their security into a manageable state. By then they were on A9.4 and they tried reporting with a third-party tool. This made it easier to produce the reports, but they still weren't getting the actionable insights that they needed.

"It was decision time," says Jen. "We could keep using our own reports and facing the same old problems; we could try and set up our own rules in A9.4, but we still didn't have a good handle on what needed to be segregated. So we decided on the other option: implement a third-party auditing solution."

The Solution

At INFOCUS 2018, Jen attended a session about QCloud, and grew excited because it seemed like the perfect solution.

"Whereas with on-premise solutions we'd have the effort and expense of installing, implementing and managing the software in-house, QCloud doesn't need any of that, and the monthly subscription is very affordable, so it was a quick and easy decision!"

"It was a real eye-opener for us, to realize how many security gaps we were overlooking because we didn't know about them."

"It tested for many things that we hadn't even considered…..QCloud shines a light on these vulnerabilities."

"It was so easy to install, and after one day's training, we were off and running! Instead of taking days to run reports and put everything together, all I have to do is request an audit, and I get the results back within 48 hours."

QCloud automates the SoD analysis using a comprehensive set of seeded rules, and Jen was surprised to see that it uncovered many issues they hadn't known about. "I was expecting maybe 400-500, but we had thousands!"

Some of these occurred because the IT team has access to all areas of the system, but others highlighted areas where non-IT users had potentially risky access combinations. "It tested for many things that we hadn't even considered. For example, why would you allow someone who can adjust inventory to key in cycle counts? Segregating those items makes sense, but there were many things like this that we simply hadn't thought of."

"Nobody wants to think that employees might abuse these capabilities, but we're responsible for protecting the company and eliminating that risk. QCloud shines a light on these vulnerabilities."

The drill-down capabilities make it easy for the controllers to see who can access what. "They login to QCloud and review the results for the users in their own Business Units. If they see that someone has inappropriate access, they just request IT to make the changes. It's very easy to understand what's causing SoD violations – you just click on the user to find out the specific rule, the applications and the security settings that are in conflict."

QCloud analysis goes a lot further than SoD. "It reports on a host of other useful items, such as users with access to Critical Objects that should be restricted, as well as many general security metrics. For example, I was surprised to see that a lot of people had Function Key security. That happened when we upgraded to A9.3. To overcome difficulties, we gave *Public to people so they could do their job, but then when you're busy you forget to go back and correct it later."

"So this was a real eye-opener for us, to realize how many security gaps we were overlooking because we didn't know about them."

Jen found that the summarized audit report was also very useful. "It's like a scorecard that shows you issues you need to clean up, and it gives you the information that you need to fix them; for example, too many people have *Public access, or these users are not assigned to any groups. And it's great to be able to demonstrate our progress when the numbers go down in subsequent audits."

The Results

- For every quarterly audit, it used to take at least five days to collate all the relevant information and produce the reports to send out to the controllers for review. Now Jen just logs in into QCloud to request an audit and the results are available within 48 hours.

- The business controllers spend much less time reviewing the reports, so they can turn them around much faster. Previously the audit cycle could take up to six weeks, with Jen hounding them to return their feedback. Last audit they all responded within a week.

- In the first 6 months of using QCloud, CTB have reduced the overall number of security issues by 50%.

- With QCloud they can analyze SoD much more rigorously and perform a comprehensive security audit across the whole system, enabling them to be proactive, rather than just focusing on the specific areas that had arisen in previous audit findings, so Jen is much more confident in the JDE security.

- Jen now feels a lot better prepared for their audits, and believes that the auditors will be impressed with the progress they've made.

"I'm ready for the next audit – bring it on!"
Jennifer Leatherman, Director of Business Systems, CTB, Inc.