CASE STUDY

AppCheck
ACCURACY IS EVERYTHING

COMPANY NAME
Rail Delivery Group

Rail Delivery Group

National Rail

Who are you?
[Tell us a bit about yourself and your organisation]

I'm Alan Cain, Head of Information Security at the Rail Delivery Group (RDG). We are a rail industry membership body that covers everything from rail settlement to timetables to everything other than driving the train.

I've worked in information security for more years than I care to remember now, and worked across lots of different industries from private sector, retail, gambling and public sector so have a vast range of experience. What I've found from that, is wherever you are and whatever you're doing, companies still have the same types of security issues.

What was the business need for AppCheck?

I had used AppCheck at another company I'd worked for previously, and when moving to RDG I noticed a lack of visibility of the applications that we use or we create. A lot of the business is outsourced which creates the issue of relying on third parties to keep things up to date like their plug-ins etc.

We wanted to be able to run ad hoc scans and see how compliant we were and identify vulnerabilities within the tools we use, this is because we don't just use them internally, we give them to the public as well. For instance, the Railcard website. Making sure these things are up to date and vulnerability free is really important to us and AppCheck was a tool I had some previous good experience with.

What were your main challenges with security before AppCheck?

It was really a lack of awareness from RDG's part where they trusted all suppliers to be up to date and have little to no vulnerabilities in their networks and applications, and for some that was true, but others might be using old code or out of date technologies.

AppCheck allows us to be able to see these vulnerabilities and be able to say to the business 'here is an insight into the security issues for this type of environment' such as Railcard for instance. We could see all the vulnerabilities relating to Railcard, we knew what needed to be changed and we could present that using an AppCheck report.

What has been the impact of using the AppCheck tool in your business?

What it did was it brought confidence into the security team. The security team are now finding and patching lots of vulnerabilities and raising awareness of them within the business where there was none before. Even that alone gave other stakeholders in the business confidence in the security team, because this is a very old industry and they aren't used to making changes so quickly. They find it hard to understand what a vulnerability is and how it works, so a tool such as AppCheck with the easy-to-read reports, looks good and allows us to present the findings in meetings.

A lot of the time there's not the internal skillset to be able to find vulnerabilities and identify critical or important ones to patch, so having a tool to present that and prioritise that helps the team focus on the right things.

CASE STUDY

AppCheck
ACCURACY IS EVERYTHING

> "AppCheck gives us the ability to quickly identify vulnerabilities and zero days, and to provide assurance to the business. "

Why AppCheck?

[What made you choose AppCheck over other vendors?]

As a former pen tester myself, I wanted a tool where I didn't have to maintain lots of different types of scripts or plug-ins. I'd used AppCheck before, so I knew it was comprehensive when it came to vulnerability discovery.

It's great for discovering vulnerabilities year-round too. You can get a pen tester to do a one-off test on your environment but in between then you want to make sure that you're keeping up to date with everything. With a tool like AppCheck you can still do the annual tests, but it makes the pen tester work a lot harder when it comes to finding vulnerabilities in your networks or your applications, because you've remediated a lot of those issues already.

What is your favourite thing about AppCheck?

I like the main dashboard which allows me to prioritise vulnerabilities and see trends and patterns.

But my absolute favourite thing is the scan templates where I can quickly see new plug-ins you've added for zero days and critical vulnerabilities. Take Sping4Shell for instance. When we asked our suppliers if our products were vulnerable, they did not really know, they had to go away and perform some research and examine the libraries used. With us, we just scanned everything and we knew immediately where we were vulnerable. Spring4Shell was a good demonstration to us of how quickly we could identify issues.

Sum up your experience with AppCheck in one line

AppCheck gives us the ability to quickly identify vulnerabilities and zero days, and to provide assurance to the business.

What are your next steps with the tool?

Aside from the day to day, we are using AppCheck for the entire business and the entire industry. So all the reports we do and vulnerabilities we discover, we formulate a single yearly report which feeds back centrally so they understand how we are approaching vulnerability management for the rail industry. We will continue to use it in this way and it's been a great addition to our security toolkit and provided some valuable insights which we've used to protect the industry.

What advice would you give to other companies looking to manage vulnerabilities?

First off, take a free scan from AppCheck. Then you can equate the risks and vulnerabilities you have to the risk appetite of the business. A lot of businesses don't really have one. They don't understand these risks or know what they are and it's hard when they can't associate vulnerabilities with the risk involved in not patching these.

A tool like AppCheck can provide a scan of your environment, and then deep dive into what the issues are and which ones are a priority. I think this would massively help a lot of companies.