COMPANY NAME

Queen's University Belfast

Can you tell us about your organisation?

Queen's University of Belfast was established in 1845, making us the UK's 9th oldest university. Today we are ranked in the top 173 universities in the world.

I am the Data Security Manager for Queen's University Belfast and run a small team, with a lot of responsibility within such a large organisation. We have more than 20,000 students, 4,000 staff and thousands of desktop computers and servers with a wide scope of technology.

Being a university, we are a magnet for hackers testing and probing and trying to compromise our system.

We needed a solution that could help lighten the vulnerability testing workload but still ensure maximum security.

Why did you choose AppCheck?

I took the free trial that you offer and tried it out. I really liked the tool and the results it brought back had a very similar output to a manual test with very professional looking reports, I would say just as professional and in depth as manual reports.

I liked the dashboards and how everything is easily visible in one place. I suppose the main thing is it's very easy to use – even to translate this to non-technical people.
I'm not very technical and I didn't struggle to get my head around it.

My opinion is that AppCheck is at least as good as manual testing and on top of this you know it's always consistent. With manual testing it depends on the capabilities of the tester but with the automated system you get that level of consistency each time.

What was the business need for AppCheck?

When I arrived at the establishment 5 years ago, pen testing was not a regular occurrence against the network, applications and infrastructure. It had been a long time since the last test.

We started with manual testing but this was very expensive, therefore we could only scope it within a limited number of targets. Being a public sector we have to go through a procurement process each time we need a test, which takes quite some time.

From my background I was aware of tools that would automatically test for vulnerabilities and this is how we came across AppCheck.

What has been the result of using AppCheck within your organisation?

AppCheck has proven to be a cost effective and time saving way to manage vulnerabilities.

A big plus point to AppCheck is that if I need to run a test, I can hit a button and spin out a test immediately without waiting for the procurement process.

We also couldn't afford to test everything manually, we were taking business time to scope out to make sure we are identifying targets that need to be tested, whereas with AppCheck we can just point AppCheck at a device or an IP address and let it work away.

AppCheck has proven to be a cost effective and time saving way to manage vulnerabilities

What were your main challenges with security before AppCheck?

The main challenge was really the cost of pen testing.

We would pay £1,000 a day for a tester and due to the size of our network, scoping tests was a challenge.

Sum up your experience with AppCheck in one line

Speed and accuracy. I can spin up a test and have a report ready for management quickly and with minimal editing.

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

I would say use this type of tool, it has a lot of advantages. We still do manual testing in line with AppCheck but we rely on this much less and it brings the costs down considerably.

I took a free test and was presented with a report I could compare to the manual test output. I was impressed with what I saw and continue to use it today, so would recommend others give this a go.

What is your favourite thing about the AppCheck tool itself?

The speed with which we can do testing – it's immediate. Just point it at the system to test and let it work away in the background. So far we have had no adverse impact on any system we have tested.

Reports are produced at the click of a button.

We had an issue with a third-party web server and we were able to set up the exact test we needed, test it and provide a comprehensive report which identified the issues with the server and begin to fix them, all within 48 hours.