Barracuda
Your journey, secured.

CASE STUDY

Leading housing association chooses SaaS-model app security.

L&Q protects apps and data in the cloud with Barracuda WAF-as-a-Service.

L&Q

A mission to protect vulnerable data

L&Q has a lot of data to protect. The charitable housing association is committed to using advanced technology to let its employees, partners, vendors, and 250,000 residents interact with the company whenever and wherever is most convenient for them via online applications. And this means that a great deal of private financial and other regulated data is carried in application traffic and stored in the company's databases. In addition, they employ an award-winning proprietary building connectivity program to remotely monitor and manage physical-plant assets such as boilers, electrical systems, plumbing, and gas systems. This IoT telemetry data traffic is significant as well, and needs to be protected against theft or sabotage.

Keeping this complex infrastructure up and running, and ensuring the security of all this data, falls—along with many other responsibilities—to Kieron Prince, L&Q's Cloud and Infrastructure Lead. "Obviously our attack surface is quite large and diverse, and our hybrid architecture adds complexity to the security challenge," he says. "Most of our workloads are still on-premises, but we are gradually transitioning to the cloud. Some on-prem workloads will remain, but we intend to migrate the majority onto Azure."

Prior to exposing each of their systems to the internet, Kieron's team performed penetration tests, and relied on application proxy appliances to keep traffic secure on a day-to-day basis. "We realized at a certain point that it was time to invest in a modern web application firewall," says Kieron. "The application proxy gave us a lot of confidence, but we began to understand that it was not really sufficient."

Profile

- Founded in 1963 in London, England
- House around 250,000 people in more than 105,000 homes
- Nonprofit organization serving diverse neighborhoods

Challenges

- Wanted to protect online application traffic with a web application firewall
- Needed a solution that would support ongoing migration from on-prem to Azure
- Was initially inclined to only consider traditional appliance solutions

Solution

- Barracuda WAF-as-a-Service

Results

- Full-featured app security across hybrid network
- Reduced IT overhead thanks to SaaS-model solution
- Ongoing cloud migration completely supported

> “Before Barracuda WAF-as-a-Service, it’s almost like we were blind. We had no visibility into just how frequently we were being probed and attacked. Now going through the logs, our eyes have been opened, and it seems a wonder that we never suffered a serious breach in the past.”
>
> **Kieron Prince**
> Cloud and Infrastructure Lead, L&Q

Stepping out of the appliance comfort zone

Among the web application firewalls that Kieron and his team evaluated, one stood out from the others as a challenge to their usual way of doing things. “I’ve always regarded a firewall of any kind as a specific appliance—a tangible asset that needs to be updated and maintained, and that depreciates over time. So it was a bit of a stretch for us to look at Barracuda WAF-as-a-Service, especially since it was a fairly new offering at the time.”

Even though it was outside his team’s comfort zone, Kieron was soon sold on the capabilities and benefits of WAF-as-a-Service. “Compared to the other solutions we looked at, WAF-as-a-Service was very simple to set up and manage,” he says. “I was already budgeting for having to hire another network engineer just to take care of a new firewall appliance, so the SaaS model starts off with a big advantage in terms of cost. And yet, despite being really easy to use, it’s fully capable. It certainly ticked all the boxes on our checklist.”

Once WAF-as-a-Service was in full production, Kieron and his team quickly came to understand how fortunate they’d been before getting a modern web application firewall. “Before Barracuda WAF-as-a-Service, it’s almost like we were blind,” says Kieron. “We had no visibility into just how frequently we were being probed and attacked. Now going through the logs, our eyes have been opened, and it seems a wonder that we never suffered a serious breach in the past.”

A solution that just works

Barracuda WAF-as-a-Service is giving Kieron and his team the confidence they need to move ahead with their cloud migration plans, free of security worries. “The Barracuda solution just seamlessly extends protection across all of our online apps, whether we host them on-prem or in Azure,” says Kieron. “Each time we migrate an app from one to the other, it’s completely effortless to have that security go along with it.”

The dependable reliability of WAF-as-a-Service is another big point in its favor. “With most technology, I take for granted that there will be problems, a certain level of frustration,” says Kieron. “With Barracuda WAF-as-a-Service, I’ve been spoiled—it’s not fair, but I’ve come to expect it to keep working flawlessly, and if something goes wrong with it, I’ll be very upset.”

Kieron sums up his experience so far: “Look, the bottom line is, I was skeptical of a SaaS model for application security. But at this point I’m very happy with it. It just goes to show that it can pay real dividends to step out of your comfort zone. In my opinion, anyone looking to invest in web application security should definitely give Barracuda WAF-as-a-Service a good long look.”

> “With most technology, I take for granted that there will be problems, a certain level of frustration. With Barracuda WAF-as-a-Service, I’ve been spoiled—it’s not fair, but I’ve come to expect it to keep working flawlessly, and if something goes wrong with it, I’ll be very upset.”
>
> **Kieron Prince**
> Cloud and Infrastructure Lead, L&Q

Please visit the Barracuda website for more information about Barracuda WAF-as-a-Service and Barracuda Cloud Application Protection.

Barracuda®
Your journey, secured.