Efinity are a software consultancy and development company with hubs in the US and the UK. They provide Quote & Bind systems for more than twenty insurance product lines.

Quote & Bind systems help insurance companies take a prospective customer from the pricing stage (quote) to the point where the coverage is in place (and thus binding). Efinity have been refining their system for more than twenty years.

Efinity’s Insurance System has everything required to run an online insurance business. The software provides instant quotes and calculates premiums for insurance policies, and has components for sales and management information. Efinity also has an insurance brokerage business, Leadenhall Underwriting, that uses their own software – so they get to experience the software as both service providers, and as service users.

Efinity deal with clients in fourteen countries. This means that the system has to deal with a lot of data, much of it personal data. The system must be watertight. In the light of recent data breaches, Efinity kept getting compliance questions from their customers: did they have the SOC 2 certification?

The SOC 2 certification is basically an audit report. When you’ve been audited, it’s proof that you have good data governance. But it takes a lot of work, because there are a lot of things you have to comply with – such as regular vulnerability scans on your infrastructure, and keeping your systems up-to-date with the latest software.
To get certified and prove their excellent governance to their customers, Efinity knew they had to find a solution to a big issue. Although they use clusters at the application level, their gateway and database nodes can’t be clustered. They run on CentOS, which gets maybe two or three critical kernel updates a month.

To get their SOC 2 certification, Efinity would have to install each update as soon as it came in, which would mean downtime for their customers, because of the reboots. They had no idea Linux kernels could be updated without rebooting, and they really did not have the bandwidth to invest in more system admin work, but they desperately wanted their servers to be compliant.

So they started Googling for a solution. And they came across KernelCare. Efinity installed KernelCare, and after a successful testing phase, they rolled it out to their production servers.

12 months on, and Efinity are fully compliant with SOC 2. A huge amount of hassle was saved by having KernelCare installed during the emergence of the Zombieload and Spectre Linux vulnerabilities.

Security is paramount in the current technological environment. Customers must trust the people they give their data to, or they will move along to the company they can trust. Getting properly audited forced Efinity to adopt KernelCare, which has not only allowed them to become fully compliant, but has enabled them to prove to their customers that they can be trusted with their data.

We tested it, but to be honest, it wasn’t very exciting—it ‘just worked’.

Andrzej Talarek
Java developer at Efinity

Automated Linux kernel security updates without reboots

KernelCare
www.kernelcare.com