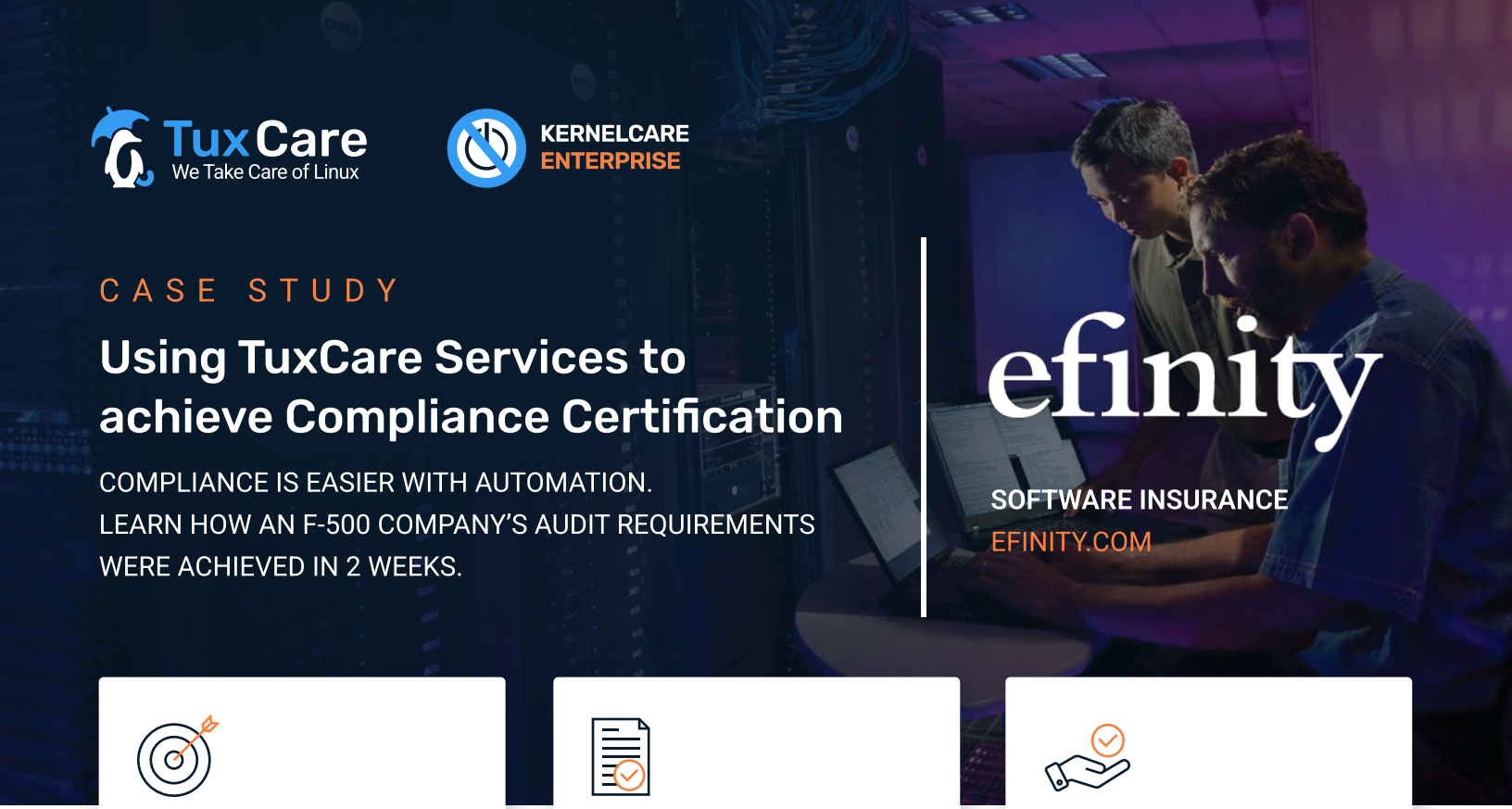
TuxCare
We Take Care of Linux

KERNELCARE
ENTERPRISE



CASE STUDY

Using TuxCare Services to achieve Compliance Certification

COMPLIANCE IS EASIER WITH AUTOMATION.
LEARN HOW AN F-500 COMPANY'S AUDIT REQUIREMENTS WERE ACHIEVED IN 2 WEEKS.

efinity

SOFTWARE INSURANCE
EFINITY.COM

The Goal

Regular security updates to Linux kernels without interruption.

The Result

To achieve SOC2 certification requirements without downtime.

TuxCare Services used by Efinity

KERNELCARE
ENTERPRISE

The Client

Efinity is a software consultancy and development company with hubs in the US and the UK. They provide Quote & Bind systems for more than 20 insurance product lines.

Efinity deals with clients in 14 countries. This means that the system has to deal with a lot of data; much of it is personal data. The system must be watertight.

The Problem

Efinity kept getting compliance questions from their customers in **the light of big data breaches**: did they have SOC2 certification?

Efinity knew they had to find a solution to a big problem to get certified and prove their excellent governance to their customers. Although they use clusters at the application level, their gateway and database nodes can't be clustered. They run on CentOS, which requires around **two or three critical kernel updates per month**.

The SOC2 certification is an audit report. When a company has been successfully audited, it proves they have good data governance. But it takes a lot of work because there are multiple regulations to comply with – such as consistent vulnerability scans on a company's infrastructure and keeping all systems up-to-date with the latest software.

Top Obstacle

To get their SOC2 certification, Efinity would have to apply each update as soon as it was available, which would mean **downtime for their customers because of reboots**. They had no idea Linux kernels could be updated without rebooting, and they did not have the

bandwidth to invest in more system admin resources. Still, they needed their servers to be compliant.

Result

Efinity reached out to TuxCare Live Pathing Services experts who helped then install KernelCare Enterprise. After a successful testing phase, they rolled this out to their production servers.

Two years on, Efinity remains fully compliant with SOC2. A considerable amount of risk and downtime was avoided by having KernelCare Enterprise installed during the emergence of the Zombieload and Spectre Linux vulnerabilities.

> **We tested it, but to be honest, it wasn't very exciting— it just worked.**

Andrej Talarek
Compliance and AWS infrastructure professional, Efinity

What this means for you:

Live patching for kernel vulnerabilities is essential for staying compliant. KernelCare Enterprise Live Patching Services automatically install Linux kernel security patches without rebooting, keeping your servers up and running constantly.

We will ensure that all the different kernels in use at your company - a mix of new, old, and custom kernels - are patched and secure against all CVEs.

KernelCare Enterprise e-Portal patch server automatically manages patch delivery, even when servers are behind a firewall and have no access to public internet.

The scanner automation ensures that reports from vulnerability scanners such as Tenable, Rapid7, and Qualys are accurate and include no false positives.

About TuxCare

TuxCare provides live security patching for critical components and extended support services for all popular Linux distributions and open source projects used by enterprises, service providers, governments, critical infrastructure operators, healthcare providers and universities all over the world.

TuxCare
We Take Care of Linux

www.tuxcare.com

r/TuxCare @TuxCare @TuxCare_ @TuxCare @TuxCare