TuxCare
We Take Care of Linux

CASE STUDY

Efinity Achieves Rebootless Vulnerability Patching to Improve Its SOC 2 Audit with TuxCare

www.tuxcare.com

Summary

Insurance management software innovator Efinity found itself with an immediate need of a SOC 2 report, for which they needed to digitally transform their vulnerability patching approach. With TuxCare's KernelCare Enterprise, Efinity was able to automatically deploy CVE patches without needing to reboot systems or schedule downtime – adding a new security component to their SOC 2 report that could impress potential customers.

Industry Insurtech, Software	
Region Global	**Founded** 2000
Headquarters Warsaw, Poland	

> **"We tested it, but to be honest, it wasn't very exciting – it just worked."**
>
> - Andrej Talarek
> Compliance and AWS Infrastructure professional, Efinity

The Challenge

Efinity is an insurance software provider that specializes in digital transformation for insurance companies, offering software solutions that insurance companies can use to modernize their own services. The organization's insurance management system is a total quote and bind solution that has racked up over 53,000 global users and generates three million insurance quotes annually across 14 countries.

In the wake of a series of large-scale, highly publicized data breaches, Efinity's customers began to approach the organization to ask about their information security practices and whether they had a SOC 2 compliance report. SOC 2 reports are generated after an in-depth auditing process that evaluates how organizations manage sensitive customer data, including the procedures they have in place and how well those procedures are followed.

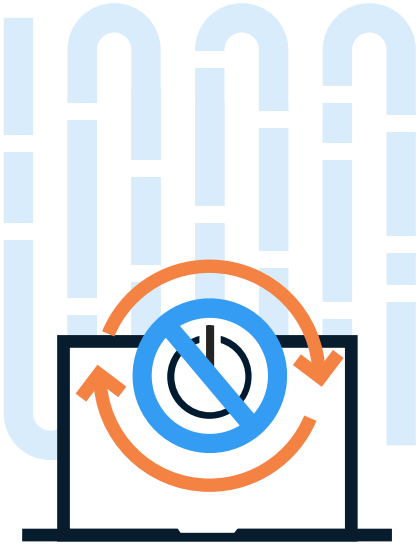
For organizations evaluating software providers like Efinity, the presence of a SOC 2 report can determine whether or not they select one vendor over another – making SOC 2 compliance a table-stakes factor for Efinity's continued success.

The Solution

To generate the best SOC 2 report possible, Efinity sought to digitally transform their approach to vulnerability management and adopt a vulnerability patching process that wouldn't require any additional system administration resources and could also help automate at least part of the process.

Efinity runs on CentOS, a community-driven enterprise Linux distribution. When a critical security update needed to be applied to their systems, they would need to reboot the Linux kernel in order to deploy a patch. Moreover, their previous patching workflow involved a number of manual processes, which they wanted to automate.

After finding TuxCare's live patching solution, KernelCare Enterprise, they discovered that they could update Linux kernels without needing to reboot – a process they didn't know was possible. With KernelCare, Efinity could also apply patches as soon as they became available, which would shrink their vulnerability exposure window and demonstrate to potential customers that their systems and data are protected.



The Results

Two years after implementing KernelCare Enterprise, Efinity remains fully compliant with the SOC 2 processes they put in place – and continues to impress potential customers with their commitment to keeping their systems patched and their user data secure.

Implementing KernelCare Enterprise meant not needing to reboot systems or schedule maintenance windows for patching-related downtime, allowing the organization to maximize system uptime and minimize service disruptions. Without a need to schedule maintenance windows to deploy patches, Efinity's team members no longer needed to perform these maintenance operations at inconvenient hours.

Additionally, with a considerably smaller patching workload, Efinity is now able to shift its IT resources to other business-critical tasks while resting assured that its systems are continually updated with the latest vulnerability patches.

Why TuxCare?

With TuxCare's family of enterprise Linux security solutions, organizations can automate vulnerability patching, minimize downtime, keep their applications secure and compliant, and get support from a team that knows Linux security best – covering their entire Linux estate, including most popular distributions, end-of-life systems, devices, libraries, and much more.

With the **KernelCare Enterprise** live patching solution, teams can put patching on autopilot for most popular distributions while avoiding downtime, disruptions, and unnecessary maintenance windows.

Extended Lifecycle Support (ELS) enables organizations to continue securely using Linux distributions and software languages that have reached end of life or no longer receive standard security support – delivering vulnerability patches for unsupported versions of CentOS, CentOS Stream, Ubuntu, Debian, Oracle Linux, PHP, and Python.

Our **Enterprise Support for AlmaLinux** offers the commercial support your business needs with break/fix support, automated live patching, extended security updates, continuous compliance, and pay-as-you-go hourly support bundles – giving you access to skilled AlmaLinux security experts whenever you need them.

With **SecureChain for Java**, companies gain access to a single trusted repository of independently verified and vulnerability-free Java packages and libraries, fully compliant with the NIST Secure Software Development Framework – so they can continue to innovate while maintaining the security of their applications.

LEARN MORE AT
www.tuxcare.com