TuxCare
We Take Care of Linux

CASE STUDY

The University of Zagreb Graduates from Disruptive Conventional Patching with TuxCare

www.tuxcare.com

Summary

Struggling with lengthy vulnerability exposure windows and too much patching-related downtime, the University of Zagreb began searching for a rebootless live patching solution. Dissatisfied with Ubuntu Livepatch, a single-distribution option, the University found KernelCare Enterprise – which enabled them to automate patching for multiple distributions while avoiding reboots, system downtime, and service disruptions.

Industry Higher Education, Research	
Region Croatia	**Founded** 1699
Headquarters Zagreb	

> **I see no alternative to the product at that level of price and reliability. We are going to stick with KernelCare Enterprise.**
>
> \- Systems Engineer at University of Zagreb

The Challenge

The University of Zagreb is the largest Croatian university and the oldest continuously operating university in all of Southeastern Europe. As an institute of higher education and a respected research hub, the University handles large volumes of sensitive data and its systems are constantly under attack from various types of cyber threats.

As a successful cyber attack could lead to data breaches that would impact future student enrollment and might even hinder research partnerships or funding opportunities, keeping vulnerabilities patched is a major priority for the University. Before finding TuxCare, however, the University's systems administration team was unhappy with its vulnerability patching approach – finding it disruptive and time consuming.

“The kernel patches needed to fix vulnerabilities were a burden to the system administration staff, in part because it brought unwanted downtime,” said one systems engineer at the University. In addition to the service interruptions their patching processes created, the team would need to take the Linux kernel offline in order to apply the patch – which meant delaying patches until they could coordinate the reboot.

These delays were sometimes unacceptably long, and ““increased the window of opportunity for the bad guys to deploy their schemes.” Faced with a continuous struggle of scheduling reboots, experiencing downtime, and operating with limited resources, the team began searching for an automated Linux kernel patching solution.

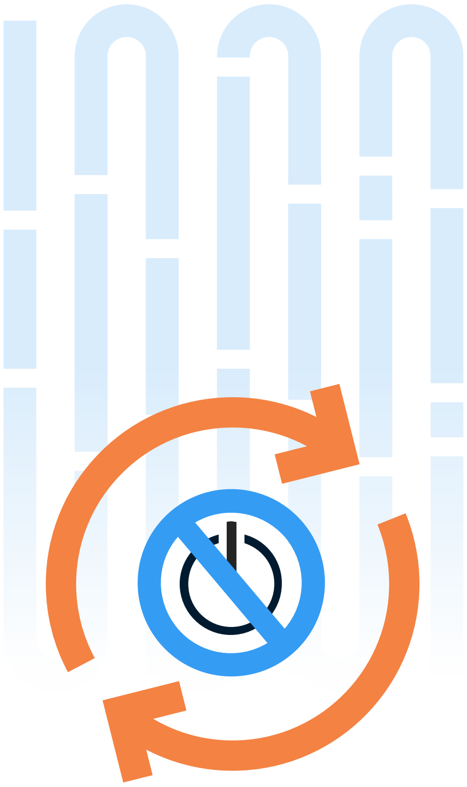
The Solution

The University of Zagreb’s search for a live patching solution first brought them to Ubuntu Livepatch, which enables organizations to patch Ubuntu servers without rebooting – but only works for Ubuntu. Because Ubuntu Livepatch didn’t support distributions outside of the Ubuntu ecosystem, the University’s Debian servers would be left out of their rebootless patches.

The University’s search continued, shifting to look for a universal live patching tool that wasn’t limited to a single distribution. Finally, they came across KernelCare Enterprise, TuxCare’s vendor-agnostic live patching solution that provides rebootless patches for all popular enterprise Linux distributions.

With KernelCare, a universal live patching solution with affordable pricing, the University could automate the deployment of CVE patches to both Debian and Ubuntu hosts without needing to reboot any systems or schedule downtime.

Looking at what KernelCare could deliver and its remarkably affordable subscription fees, the University’s systems administration staff decided to sign up for a test account right away – without even waiting for funding approval. In fact, they were so thrilled to get started that they made their initial payment with a personal PayPal account so that they could begin live patching as quickly as possible.



The Results

After implementing KernelCare Enterprise for a brief trial , the University quickly noticed how well the solution worked in continuously deploying the latest Linux kernel patches without requiring any reboots or downtime.

Installing the solution was simple as well, only requiring the team to run a script – a process that can be automated across large server fleets. Soon after their trial period began, with the flick of a switch, the team activated KernelCare Enterprise across its entire server environment.

Interestingly, one point quickly emerged. The team was surprised to find out that their "fully patched" Debian Jessie servers had 91 vulnerabilities. Thankfully, this was rapidly and effortlessly patched with KernelCare Enterprise.

> **“The TuxCare support team has been very open to suggestions to improve an already excellent service, and I feel almost like a part of the developer team.”**

On top of immediately running smoothly, KernelCare Enterprise showed no signs of glitches, from testing on through to rollout. Now able to avoid patching-related maintenance windows entirely, the team no longer needed to write long, apologetic emails that non-technical users wouldn't understand anyway. Moreover, there were no longer any end-user service disruptions.

The University’s systems administration staff was thrilled with the level of customer support they received from TuxCare, with support engineers responding to requests within tens of minutes and solving issues within hours. “The TuxCare support team has been very open to suggestions to improve an already excellent service, and I feel almost like a part of the developer team.”

Now, two years after implementing KernelCare Enterprise, one of the University's system engineers says that they're thrilled to keep using TuxCare's technology, especially with how superior the product is compared to other live patching solutions. "I see no alternative to the product at that level of price and reliability. We are going to stick with KernelCare Enterprise."

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