TuxCare
We Take Care of Linux

CASE STUDY

OCLC Puts an End to Patching Outages & Reduces CVE Exposure by 90% with TuxCare

www.tuxcare.com

Summary

After implementing TuxCare's automated live patching solution, OCLC eliminated the need for patching-related system outages while reducing the organization's patching workload by 72% and shrinking its vulnerability exposure window by 90%.

Industry Information, Library Software	
Region Global	**Founded** 1967
Headquarters Dublin, Ohio	

> **"Things are going well. We're doing monthly patching with KernelCare and it's operating as expected. No downtime. No outages. Reduced management time."**

The Challenge

OCLC, Inc. is a global cooperative that provides shared technology services, original research, and community programs for libraries around the world. Widely known for its international WorldCat library catalog and maintaining the Dewey Decimal Classification system, the organization also sells a number of software solutions.

With several teams around the world administering roughly ten thousand systems that mostly run Red Hat Enterprise Linux (and a few CentOS boxes), applying vulnerability patches was a continuous challenge for OCLC. Given the geographic distribution of their teams, scheduling and executing the required reboot cycle was difficult – particularly when trying to keep maintenance windows to a minimum.

The Solution

To solve their patching-related operational inefficiencies, OCLC decided to begin testing and mapping out the implementation of TuxCare's KernelCare Enterprise, which would enable them to automatically deploy CVE patches without rebooting and thus accelerate their patching lifecycle.

To start, they opted to deploy KernelCare to just their production environment, which would cover 4,000-5,000 systems – including some FedRamp systems that involved some especially strict standards that they'd need to adhere to.

At the time, the organization was contending with a particularly problematic group of systems that was causing consistent friction. While mapping out the initial deployment of KernelCare, they made a decision: if TuxCare's solution could reduce the impact of these problematic systems, they would deploy KernelCare Enterprise and the LibCare add-on (for live patching shared libraries) to the rest of their Linux hosts – totaling roughly ten thousand systems.

The Results

After seeing the efficiencies generated by KernelCare Enterprise within their production environment, OCLC opted to deploy it to all of their Linux hosts. To quantify the impact of TuxCare's automated live patching solution, the organization began to run an internal study to measure the impact of KernelCare Enterprise on its operational efficiency.

The outcomes were significant. Before adopting a live patching approach, OCLC underwent 73 outages due to vulnerability patching in just 12 months. After implementing TuxCare, the company experienced zero patching-related outages – a 100% reduction in downtime due to patching.

Their internal study also found that TuxCare enabled their teams to substantially bring down the number of hours they were collectively dedicating to CVE patching by 72%. Additionally, their vulnerability exposure window contracted by about 90% – from 115 days down to only 12 days.

"With KernelCare, we've reduced our patching-related outages from 73 per year down to zero, we've slashed the hours we spend on CVE patching by 72%, and our vulnerability exposure window has shrunk from 115 days to just 12 days."

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

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

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