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 offers 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.

After deploying KernelCare into their development environment followed by two other non-production environments, they opted to deploy the solution into 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 with TuxCare, OCLC was experiencing outages caused by executing reboots to apply vulnerability patches. After implementing TuxCare, the company stopped experiencing these outages entirely – achieving a 100% reduction in downtime due to patching-related reboots.

> “With KernelCare, we've completely eliminated patching-related downtime, we've slashed the hours we spend on CVE patching by 72%, and our vulnerability exposure window has shrunk by 90%.”

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%.

Why TuxCare?

Waiting to apply security patches until you're ready to restart systems and devices is leaving your organization vulnerable and putting your compliance posture at risk. TuxCare's live patching solutions protect your Linux systems by rapidly eliminating vulnerabilities with no need to wait for maintenance windows or downtime. With TuxCare, IT teams can automate the process of taking new patches through staging, testing, and production on all popular Linux distributions.

TuxCare features flawless interoperability with vulnerability scanners, security sensors, and automation and reporting tools, as well as our ePortal management platform – a dedicated private patch server that runs inside your firewall on premise or in the cloud. TuxCare is the only provider that can live patch all vulnerabilities in kernels, shared libraries, virtualization platforms, and open-source databases across all popular distributions.

LEARN MORE AT
www.tuxcare.com/live-patching-services