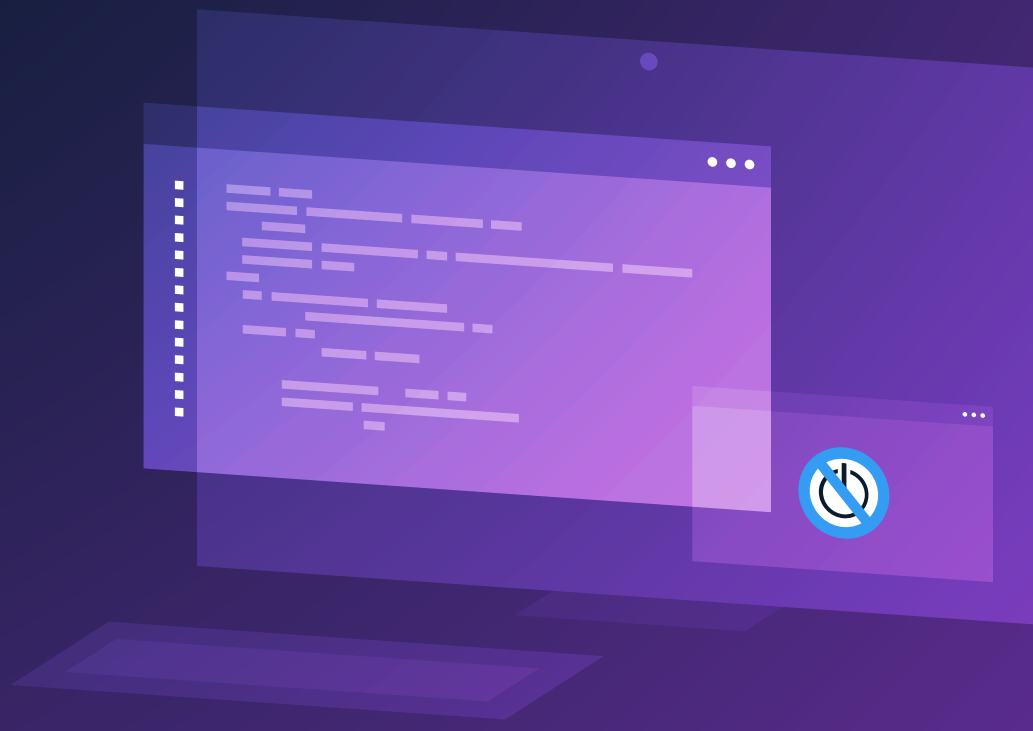
Guide

TuxCare

Patching in the Background:

Avoiding IT Burnout with Automated Live Patching

How IT managers minimize their team's patching-related working hours and relieve stress by putting Linux security patching on autopilot with live patching – a non-disruptive approach that applies patches to running systems without downtime, making it easier to maintain security and compliance.



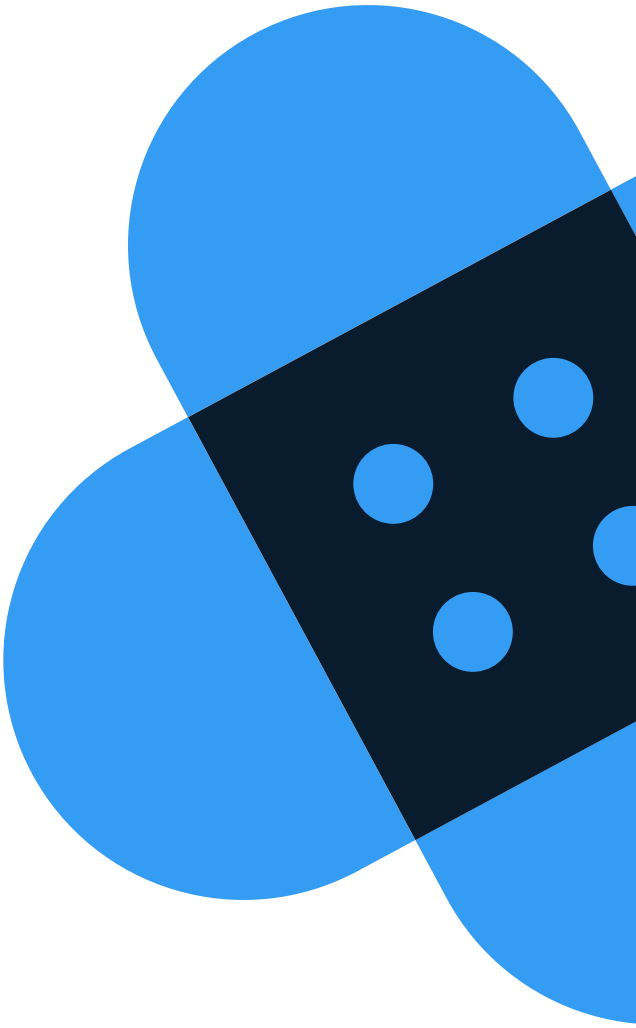


Table of Contents

Traditional Patching: A Never-Ending Headache for IT Teams

For anyone that works in enterprise IT, the burden of being responsible for Linux security patching has likely been a persistent challenge. Not only is there a constantly looming threat of increasingly sophisticated cyber attacks, but the conventional process of patching Linux vulnerabilities is time consuming – making it difficult to apply patches within time limits mandated by certain types of compliance.

In conventional Linux kernel patching, the system needs to undergo a reboot – a process that often requires IT Managers to assign team members to babysit until it's finished, often during off-peak hours and weekends. Coordinating these reboots among different departments can be a logistical nightmare, and the difficulty of scheduling downtime before compliance deadlines means that non-compliance penalties are also a constant danger.

Moreover, delaying patches to accommodate reboot schedules can leave systems vulnerable to security threats. This cumbersome process not only wastes valuable IT time but also increases the risk of potential exploitation during the window of vulnerability.

Fortunately, with a modernized Linux vulnerability patching approach called "live patching," IT teams can focus on developing and deploying new technologies rather than babysitting existing ones – all while making it easier to demonstrate compliance and minimize the risk of vulnerability exploits.

What Is Linux Live Patching?

With the downtime, disruptions, inefficiencies, and risk of non-compliance that the conventional vulnerability patching approach introduces, IT teams at many of the world's most innovative organizations have adopted live patching.

> **Live patching is an automated, non-disruptive patching approach that doesn't require reboots, downtime, or manual patching workflows. With a live patching solution, all the latest patches are automatically applied in the background, while systems are running, so that teams can "set it and forget it" while focusing their attention on other important tasks.**

After companies adopt live patching, there's no more babysitting reboots, interrupting important long-running operations, scheduling inconvenient maintenance windows across multiple departments, or wasting your team's time on an outdated security approach.

The ability to deploy security patches without disruptions as soon as they are available not only reduces unnecessary patch delays and helps companies stay compliant with regulatory patching requirements, but also enables organizations to completely avoid reboots. Some companies that use KernelCare Enterprise live patching, for example, have been able to keep their systems patched without rebooting for over eight years.

The Benefits of Live Patching

Reduce Risk

Patching Linux kernel vulnerabilities quickly after patches are released allows your organization to minimize the window of opportunity for malicious entities to exploit them

Patch Faster

Deploy security patches as soon as they're available, automatically – without disruptions or delays – so that you don't need to wait for a hard-to-coordinate maintenance operation

Stay Compliant

By accelerating your patching timeline, you'll make it easier to comply with regulatory regimes that require companies to patch within a certain amount of time after a patch becomes available

Minimize Downtime

By eliminating the need for system reboots, live patching ensures near-constant system availability, which is crucial for businesses that require 24/7 uptime.

Boost Productivity

By leaving behind the conventional patching approach, which isn't an efficient use of time or resources, your team will have more time to spend on other critical tasks

How Live Patching Works

Live patching with KernelCare Enterprise replaces code that contains vulnerabilities with new, secure code while your Linux kernel is running – eliminating the need for a system reboot.

The KernelCare Enterprise live patching process looks like this:

1

We Create the Patch

We create code that patches insecure kernel code with a secure but functionally equivalent replacement.

2

We Prepare the Patch for Deployment

We compile every patch that impacts the affected kernel and deploy it to our distribution servers.

3

You Receive the Patch

A KernelCare process running on your server checks our distribution servers every 4 hours. If a new patch is available, it can then be downloaded and applied to your running kernel – a process that can be automated.

4

KernelCare Applies the Patch

The patch is passed to the KCE kernel module, which – in a matter of nanoseconds – pauses all processes, loads the updated binary into the secure kernel space, redirects all functions to the updated code – and the kernel resumes. Because this happens in nanoseconds, no processes are interrupted, and no failover condition is ever triggered.

And that's it!

Did you know that KernelCare Enterprise live patching is compatible with most popular Linux distributions, including Debian, Red Hat Enterprise Linux, CentOS, Ubuntu, AlmaLinux, Oracle Linux, and many more?

Live Patching Beyond the Linux Kernel

In addition to patching the Linux kernel, live patching can be applied to other critical areas of your organization's Linux estate.

Unlike most live patching providers, KernelCare Enterprise can be extended to shared libraries, IoT environments, and QEMU-based virtualization systems.

LibCare	Minimize downtime and automate vulnerability patching for OpenSSL and glibc without needing to reboot systems or schedule maintenance windows
IoT Connected Devices	Patch your Linux-based enterprise Internet of Things (IoT) ecosystem without needing to take connected devices out of production
QEMU-based Virtualization Systems	Stay patched without needing to shut down or migrate the virtualization layer or reboot the hypervisor

Is Live Patching Right for Your Team?

While the benefits are clear, implementing live patching depends on the needs of your organization and your IT team, specifically. Factors such as the criticality of continuous uptime, the scale of your operations, and regulatory requirements should all be considered. For organizations with 24/7 operations or those under stringent compliance regulations, live patching can be a game-changer.

By integrating live patching into your organization's software maintenance and cybersecurity strategy, you can significantly enhance system availability, security, and overall business continuity.

There are a few Linux live patching solutions out there. KernelCare Enterprise delivers live patches to most popular enterprise Linux distributions at a fraction of the cost of premium support services from vendors like Canonical, Red Hat, and Oracle – which may also only support one or a few Linux distributions.

If you already have a premium support subscription from a major Linux distribution vendor, live patching with those costlier options may be a better option for your organization. If you want to spend less on non-disruptive live patching or run a Linux estate with multiple distributions, KernelCare Enterprise is likely the best option.

To start a free trial of KernelCare Enterprise, get a quote, or ask one of our Linux security experts a question about live patching, visit our website.

www.TuxCare.com