TuxCare
We Take Care of Linux

GUIDE

What Is Live Patching?

The Ultimate Guide to Automated, Rebootless Linux Vulnerability Patching

An introduction to live patching, an innovative Linux vulnerability patching approach that requires neither reboots nor downtime – enabling organizations to put security patches on autopilot, minimize disruptions, and maintain compliance.

www.tuxcare.com

It’s Time to Modernize Your Linux Security

Contents

What Is Linux Live Patching?

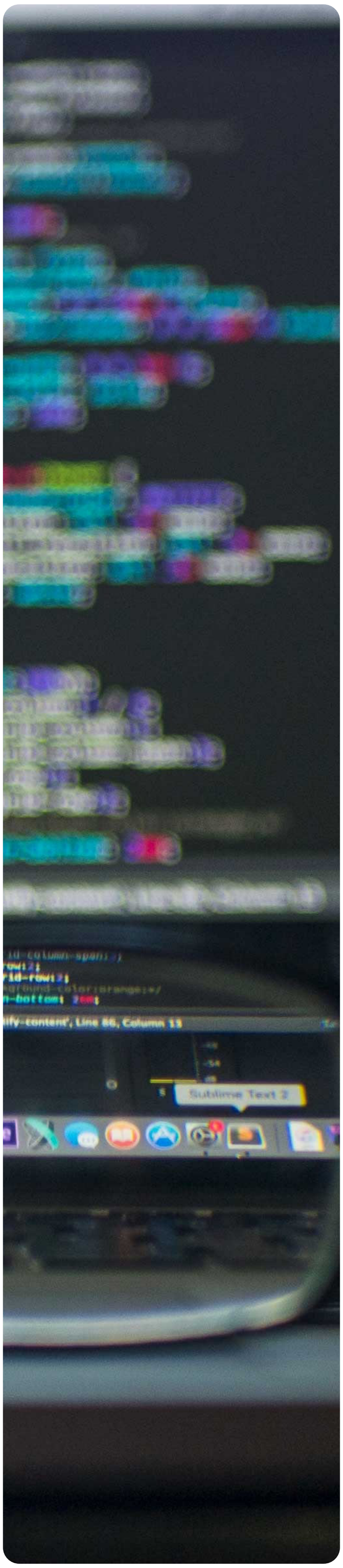
Conventional vulnerability patching for the Linux kernel, which remedies security issues to prevent damaging cyber attacks, requires a system reboot to load the patched code into the kernel. Because a reboot is needed, the process often involves coordinating a maintenance operation among multiple stakeholders, scheduling this maintenance window at a time when system disruption will be less impactful, and assigning team members to babysit a lengthy system reboot.

This conventional approach can reduce system uptime, take time away from other important tasks, hurt revenue generation, and negatively impact the customer experience.

For these reasons, innovative organizations around the world have adopted live patching – an automated, non-disruptive patching approach that doesn't require reboots, downtime, or manual patching workflows.

With live patching, IT, DevOps, and SOC teams can put their Linux security patching on autopilot and deploy all the latest patches as soon as they become available – all taking place in the background, while systems are running. After companies adopt live patching, there's no more babysitting reboots, interrupting important long-running operations, scheduling inconvenient maintenance windows, or wasting your team's time on an outdated patching technique.

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

> 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%.
>
> OCLC

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, databases, 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

Databases

Keep your databases secure without disrupting service or impacting query performance

> "It's been a real pleasure to work with TuxCare to take care of required cybersecurity updates on some of our servers. The product and the people have been great, we found it easy to implement, and it works great.
>
> ALVARIA®

Is Live Patching Right for Your Organization?

While the benefits are clear, implementing live patching depends on the specific needs of your organization. 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 get a quick, personalized demo of KernelCare Enterprise or ask any questions you may have about live patching, reach out to a TuxCare Linux security expert.

LEARN MORE AT
https://tuxcare.com/live-patching-services/