TuxCare
We Take Care of Linux

DATASHEET

KernelCare Enterprise Live Patching

Minimize risk while maximizing the availability of your Linux systems

www.tuxcare.com

About KernelCare Enterprise Live Patching

Security operations teams strive to minimize their organizations' risk by identifying vulnerabilities[1] and setting a patching policy to address them. At the same time, system owners strive to provide a great user and customer experience by making the most of their available systems. This is sometimes seen as a tradeoff, with some organizations accepting a higher level of data breach risk to support operations and provide a better customer experience. Meanwhile, other organizations opt to reduce their risk by updating their systems more frequently at the cost of using more IT resources and often while undermining their customer experience.

Industry leaders do not make this tradeoff. Instead, thanks to live patching technology, they provide their users with continuous service while at the same time reducing their risk and rapidly patching all vulnerabilities – all with no additional effort.

Reduce vulnerability patching time and risk

Eliminate downtime; patch kernel and critical components while the system is running

Patch all vulnerabilities and avoid lengthy risk analysis

KernelCare live patching enhances your vulnerability patching program by reducing the vulnerability window, eliminating downtime, and erasing the hidden costs of maintenance windows. With KernelCare, systems are patched in milliseconds while they're still running, eliminating vulnerability patching delays caused by the wait to the next maintenance window. The kernel and processes running in the system are updated to non-vulnerable code automatically with no downtime.

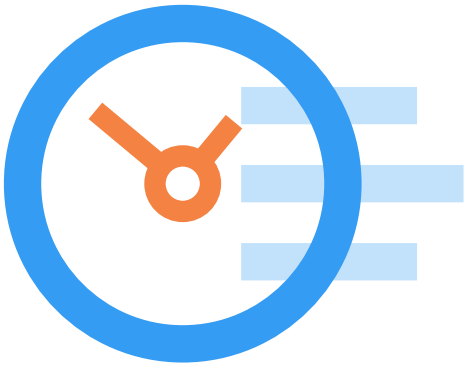
The following information will help you understand not only how KernelCare live patching helps you achieve your vulnerability patching goals and eliminate time spent in system maintenance, but also how this solution enables you to reduce the overall costs of your vulnerability patching program.

[1] Exploitation of vulnerabilities is the main path to a ransomware incident and the second reason for a data breach in a web application, according to Verizon's Data Breach Investigations report for 2022.

Key Benefits

Accelerate your vulnerability patching timeline

In large organizations, the separation of duties and different system ownership make security patching a challenging task. According to Ponemon Institute, 56% of enterprise organizations take from five weeks to more than one year to apply security patches. At the same time, high risk vulnerabilities appear at unexpected times. Instead of spending time identifying the responsible teams and deliberating on patching and restarting the vulnerable servers during the next maintenance window, KernelCare live patching enables you to patch systems immediately – shrinking the vulnerability patching window to the absolute minimum. Any vulnerable servers are patched as soon as the fix is available.



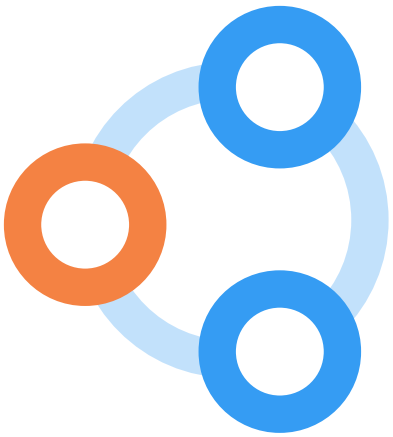
Eliminate maintenance windows or set the right one for your organization

Several organizations have settled for monthly or quarterly maintenance windows where services are restarted and servers are rebooted. This way, systems include the latest vulnerability fixes – not only at the cost of service downtime, but also at the expense of wasting human capital on mundane tasks. With KernelCare, you can eliminate maintenance windows entirely or set them to what makes the most sense for your business, whether it is 12 months apart or after several years of uptime. You're now able to eradicate downtime from your infrastructure and use your engineers where they're needed most, all while automatically live patching vulnerabilities.

Avoid lengthy risk analysis with wide vulnerability coverage

When KernelCare Enterprise is combined with the LibCare add-on, all vulnerability fixes available to your Linux kernel are live patched as well as glibc and OpenSSL libraries. This includes all vulnerabilities irrespective of their CVSS score, as CVSS score does not translate to risk level for every possible environment. Now, you can avoid lengthy vulnerability impact analysis as well as false alarms. With KernelCare Enterprise there is no vulnerability-related reason to reboot a KernelCare live-patched system – EVER. Our customers have kept their systems running for more than 8 years with zero downtime and have all available vulnerability patches applied.

Patch all the Linux systems in your infrastructure



KernelCare live patching is available for a variety of Linux systems. Whether you have infrastructure with CentOS, AlmaLinux, Rocky, Red Hat Enterprise Linux, Amazon Linux, Oracle Linux, or Ubuntu systems, KernelCare Enterprise will patch your systems. It is available for both x86-64 (Intel and AMD) and ARM64 architecture. On each supported system, all the released kernels receive security patches for a practically unlimited period of time.

The extensive list of all supported systems is available at: https://patches.kernelcare.com/

Follow your organizational patch deployment policy

Several organizations have a gradual patch roll-out policy or maintain a strict policy on which systems get upgraded and when. With the on-prem KernelCare ePortal, a private patch server for gated infrastructures, you can use the patch roll-out policy of your choice while automatically deploying patches in your air-gapped environment – all with a simple user interface.

Questions

Does KernelCare live patching apply to CentOS, AlmaLinux, or Rocky Linux?

Several organizations do not require support for their operating systems and are content with an enterprise Linux distribution without support. KernelCare live patching is not only practical for these systems, but also adds significant value by eliminating unnecessary maintenance processes and reducing the vulnerability window caused by delaying patching until the next maintenance window.

How does KernelCare live patching compare to the feature bundled in my OS?

Comparison with Oracle Linux live patching

Oracle Linux provides live patching with premium subscriptions only. By using KernelCare live patching, there is no need to use the premium subscription, saving you more than $1000 per year per host. At the same time, KernelCare enables you to patch more security vulnerabilities for both x86-64 and ARM64 for a practically unlimited period of time.

Comparison with Ubuntu and Red Hat Enterprise Linux live patching

Both Red Hat Enterprise Linux and Ubuntu live patch certain vulnerabilities of high and critical severity only. The kernels are live patched for 3–6 months, after which the system must be rebooted with the latest kernel to receive live patches again. KernelCare, on the other hand, increases your vulnerability patch coverage to all vulnerability fixes irrespective of severity. All vulnerabilities, including those rated with a medium CVSSv3 score, are patched. At the same time, KernelCare releases live patches for a practically unlimited timeframe, enabling you to get the most out of your systems without reboots for years.

	Canonical Ubuntu	Red Hat Enterprise Linux	Oracle Linux	**KernelCare Enterprise with LibCare add-on**
Technology	Livepatch	Kpatch	ksplice	**KernelCare**
Architectures	x86-64	x86-64	x86-64, ARM64	**x86-64, ARM64**
Coverage	Linux kernel	Linux kernel	Linux kernel & critical userspace	**Linux kernel & critical userspace**
Systems available	Selected Ubuntu LTS kernels	Red Hat Enterprise Linux kernels	Oracle Linux & selected kernels	**Vendor independent**
Vulnerabilities patched	Subset of High & Critical	Subset of High & Critical	High & Critical	**All[2]**
Kernel patching lifetime	3–6 months	6 months	Practically unlimited	**Practically unlimited**
Price	Bundled in Ubuntu Advantage $225 / year per host	Bundled in Red Hat subscription $349 / year per CPU socket	Bundled in Oracle Premier subscription $2299 / year per host	**$94 per year per host**

Get Started with KernelCare Enterprise

Reaching this point demonstrates that improving your vulnerability patching process is important to you. To learn more about minimizing your vulnerability risk and accelerating your patching time by adopting a live patching approach, follow the links below to chat with one of our experts.

TALK TO AN EXPERT

LEARN MORE

[2] We patch every vulnerability that poses a threat of exploitation, regardless of CVSS score.