TuxCare
We Take Care of Linux

DATASHEET

KernelCare Enterprise Live Patching

Minimize risk while maximizing the availability of your Linux systems

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.

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 automatically 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 while they run.

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

Key Benefits

Automate your vulnerability patching and reduce the vulnerability window

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 and cybersecurity frameworks require automated patch management to defend against them. 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 automatically as soon as the fix is available in accordance with your organization's patch deployment policy.

Reduce workload with wide vulnerability coverage and integration

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 system components. This includes all vulnerabilities irrespective of their CVSS score, as CVSS score does not translate to risk level for every possible environment.

[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.

This significantly reduces the time spent in analyzing system vulnerability data by making sure that these vulnerabilities do not show up at all in your vulnerability scanner. KernelCare Enterprise integrates with all major vulnerability scanners, including Nessus, Qualys, Rapid7, Puppet, Ansible, Chef, Datadog, Tanium, and Crowdstrike.

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.

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.

	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**

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

Pricing

To learn more about minimizing your vulnerability risk and accelerating your patching timelines, follow the links below to chat with one of our experts.

Talk to an expert
tuxcare.com/talk-to-an-expert

Learn more
tuxcare.com/live-patching-services

Follow TuxCare on Social Media

☎ +1 (800) 231-7307 ✉ sales@tuxcare.com