Data Sheet

SUSE® Linux Enterprise Live Patching

Downtime is expensive, even when it is planned. Live Patching virtually eliminates the need for downtime—and allows for easier planning of scheduled downtime—by applying critical Linux fixes outside of maintenance windows. Live Patching offers a proactive and dynamic approach to Linux kernel and Linux executable maintenance that saves your company valuable time and money by never needing to stop the kernel or applications.

SUSE

07.06.2022

Product overview

SUSE® Linux Enterprise Live Patching is a simple open source solution that delivers live kernel patching without the need to reboot. With this subscription offering based on the kGraft project, you can perform patching without interrupting your mission-critical workloads and in-memory databases, saving the cost of downtime and increasing service availability. Because it builds on to the existing SUSE Linux Enterprise kernel infrastructure and uses familiar deployment methods, Live Patching is an easy way to make operating system maintenance more efficient and secure.

Live Patching puts you in charge of your kernel updates and service availability. Even when urgent kernel updates are needed, SUSE Linux Enterprise Server can run continuously—with zero execution interruptions, not even a millisecond—while you apply critical kernel patches in the background.

In addition to Linux kernel maintenance, you can live patch updates for user space processes and libraries, enabling you to deliver live patches to any of your Linux executables or libraries at runtime, without the need for restarting those applications. This can be used to perform critical security updates and/or serious bug fixes on the fly to avoid interruption of service.

Key benefits

SUSE Linux Enterprise Live Patching keeps your systems running smoothly and securely on the front end while critical updates are applied on the back end.

- **Reduce downtime**—You can reduce downtimes whether planned or unplanned. In the case of unplanned downtimes, you can potentially eliminate them as you do not need to reboot the system when you apply kernel patches. You will also save time and resources by avoiding the need to plan for resources to handle unplanned downtime. In the case of planned downtimes, you can reduce the duration of the planned downtime by saving the time in rebooting the systems since there is no need to reboot the system when you apply kernel patches with Live Patching.
- **Increase service availability**—Live Patching technology allows you to apply critical kernel patches with zero interruption of user applications and kernel execution as a result you can maintain continuity of service at all times. For memory database applications such as SAP HANA that may need a long time for a complete reboot cycle after the application of kernel patch, you can save hours of time by avoiding kernel reboot with Live Patching.
- **Enhance security and compliance**—You can enhance security by applying security patches when needed and not waiting for the maintenance window or planned downtime to apply a critical kernel security patch with zero interruption to your running workloads. You can also help the compliance and auditing efforts with the ability to review the source code of patch when

"SUSE Linux Enterprise Live Patching provides a stream of packages to update a running kernel without interruption. With this subscription offering from SUSE, you can perform patching without rebooting your system, saving the cost of downtime and increasing service availability."

applying patches. No other product offers this capability.

- **Increase service availability**—Live Patching technology allows you to apply critical kernel patches with zero interruption of user applications and kernel execution as a result you can maintain continuity of service at all times. For memory database applications such as SAP HANA that may need a long time for a complete reboot cycle after the application of kernel patch, you can save hours of time by avoiding kernel reboot with Live Patching.
- **Enhance security and compliance**—You can enhance security by applying security patches when needed and not waiting for the maintenance window or planned downtime to apply a critical kernel security patch with zero interruption to your running workloads. You can also help the compliance and auditing efforts with the ability to review the source code of patch when applying patches. No other product offers this capability.

Key features

- **Zero execution interruption**—Stopping the kernel is problematic for low-latency applications such as transactional databases. Live Patching doesn't stop the system during patching. The patching infrastructure is built directly in to SUSE Linux Enterprise Server 12 and SUSE Linux Enterprise Server 15. Live Patching uses the familiar ftrace-based approach to perform the updates. This happens without ever stopping the kernel, not even for a moment.
- **Minimalist design**—Live Patching is easy to add to your existing code base. It consists of only a small amount of code because it leverages the technologies and ideas already present in the upstream Linux kernel: ftrace and its mcount-based space allocation in function prologues, the INT3/IPI-NMI patching also used in jump labels and read-copy-update (RCU)-like code updating that does not require kernel stoppage. A kernel live patch is a kernel module and relies on the in-kernel module loader to link the new code with the kernel.
- **Security**—The Live Patching kernel module is signed by SUSE. This approach complies with advanced security technologies such as UEFI secure boot, which require kernel modules to be signed by an approved signing key. Via this signature, you can minimize your exposure to security risks by verifying that a kernel

live patch has been created by SUSE.
- **Familiar deployment methods**—Like all maintenance updates, the patches delivered by Live Patching are delivered as signed RPMs. Introducing the solution into your established administrative process is simple because you can reuse existing deployment methods, including but not limited to YaST®, zypper, SMT and SUSE Manager.

System requirements

Minimum requirements:

- A system that runs SUSE Linux Enterprise Server 12 or 15
- Zypper must be installed and configured to receive updates

Supported processor platforms:

- x86-64
- ppc64le (IBM Power Systems)
- IBM Z and LinuxONE

For detailed product specifications and system requirements, visit: https://www.suse.com/products/live-patching/

Contact your local SUSE Solutions Provider, or call SUSE at:

1 800 796 3700 U.S./Canada
1 801 861 4500 Worldwide

SUSE
1800 S. Novell Place
Provo, UT 84606

SUSE
Maxfeldstrasse 5
90409 Nuremberg
Germany

SUSE

2022

SUSE
Maxfeldstrasse 5
90409 Nuremberg
www.suse.com

For more information, contact SUSE at:
+1 800 796 3700 (U.S./Canada)
+49 (0)911-740 53-0 (Worldwide)

Innovate Everywhere