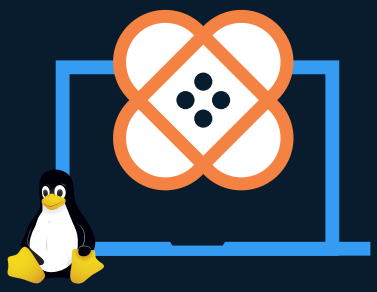
TuxCare

LIVE PATCHING FOR ENTERPRISE LINUX

Temporary vs. Persistent Patching

Which of these two methods of “live patching” (patching vulnerabilities without a reboot) is better for keeping enterprise Linux servers secure with as little downtime as possible?



The Temporary Method

The temporary method is also called “stack” patching because temporary patches pile up over time, degrading performance and stability – for which the only solution is to reboot the server to load a fresh kernel into memory. So, while this approach applies a patch without an initial reboot, it actually does involve a server reboot and downtime later on.

Temporary live patching requires package management software to be installed on the server, only applying patches according to the update workflows specified by the user.

The Persistent Method

In persistent live patching, which requires no reboot at all, a kernel module periodically checks a dedicated patch server for new patches and applies any new ones that have been released. These patches are “monolithic,” not temporary, because each patch fixes all previous CVEs affecting the kernel.

With no reboots, this method enables servers to stay up and running essentially forever – with many enterprises not needing to reboot servers for over 5 years while still running fully patched kernels.

What About Costs?

Temporary live patching is included with some Linux OS distributions and with some vendors’ support contracts, but shouldn’t be considered free or inexpensive, because – on top of subscription expenses – it incurs additional costs in time and trouble that aren’t apparent upfront

Persistent live patching can be provided by a vendor at a lower cost than manufacturer-specific temporary live patching solutions, while also replacing manual workflows with automated processes – **minimizing the time and effort required to patch Linux servers** on a variety of distributions.

Which Method Is Best?

For an organization that runs a limited number of servers for internal use, the temporary method of live patching may work ok. If your IT staff and budget are big enough so that cost and efficiency aren’t pressing concerns, the manual management and reboots associated with this method will present no problems.

For enterprises that want to reduce manual workflows, minimize end-user disruptions, shrink patching-related costs, and avoid downtime associated with rebooting, then persistent live patching is the way to go.

About TuxCare

TuxCare provides persistent live patching for all popular Linux distributions and open-source projects, enabling organizations to keep their systems secure with **zero patching-related reboots, downtime, or maintenance windows**. In addition, TuxCare offers live patching for end-of-life Linux, keeping systems fully patched for years after the vendor-supported lifecycle or a variety of distributions and software languages.