KernelCare

How KernelCare Works

Rebooting Hurts

Rebooting your servers hurts your customers and hurts you. It is often done deep in the night to minimize the impact on peak-time services. It forces downtime on you and your business. A server reboot can take 15 minutes or more to complete. It can take even longer for performance to stabilize and for you to confirm all services are running. Rebooting is not something you want to do often. But a reboot is the only way to apply patches for kernel security vulnerabilities.

Until now.

Now there is KernelCare. It automatically patches kernel security vulnerabilities without rebooting. No downtime, no interruption of service.

KernelCare

Preparing a Patch

Our kernel team monitors security mailing lists. When a vulnerability affecting supported kernels is announced, we prepare a patch immediately. We compile each patch for that kernel and deploy it to our *distribution servers*.

A *KernelCare agent* process running on your server synchronizes and checks with our distribution servers every 4 hours. If a new patch is available for the active kernel, the agent downloads it and applies it to the running kernel. Your kernel is secure again.

How Patches Work

When we discover a vulnerability, we create a “patch”. This is code that *patches* insecure kernel code with a secure but functionally equivalent replacement.

In the simplest case, patching can mean the modification of a single line of code. In others, more complex mitigation may be necessary, such as the addition of missing checks, changes to data structure or functions.

We compile patched code as usual, adding information about what has changed and how to apply it.

Special Kernel Module Applies Patches

To apply patches, a special *KernelCare kernel module* is used. It loads the update into kernel address space, sets relocations (i.e. fixes references to original kernel code and data) and safely switches the execution path from original to updated code blocks. It is important to apply changes correctly and KernelCare does just that. It makes sure the CPU does not execute any original code blocks when switching to the new version.

Allocates kernel memory, loads new, secure code into it

Momentarily pauses all processes in a 'safe' mode

Modifies original functions and jumps to new secure code, ensuring old (vulnerable) code can never run

Unpauses all processes and resumes

KernelCare

It Does It Super-fast

An instantaneous update process of applying patches means **no downtime, no service interruptions or packet drops**. Everything continues to operate as before, with all vulnerabilities gone.

KernelCare

To learn more about **KernelCare,**
visit https://www.kernelcare.com/

Questions? Contact Our Sales Team:
+1 (800) 231-7307 | sales@kernelcare.com

300K+
servers running securely without reboots with KernelCare

KernelCare is a product of CloudLinux, the company that is making Linux secure, stable and profitable since 2009. Its flagship **CloudLinux OS powers over 20 million websites**.