KernelCare

Live Linux Kernel Vulnerability Patching with No Reboots. Ever.

Powers 300K+ servers, trusted by 1,500+ Enterprises

What is the Problem?

For servers to be secure, kernels must be *up to date*. This requires frequent *updates and reboots*.

- Unpatched kernels make servers vulnerable to attacks;
- Enterprises often wait weeks or months until the next scheduled reboot cycle;
- Delays lead to compliance issues and critical security risks.

KernelCare

Rebooting Your Servers is Making You Insecure and Noncompliant.

(and it's a matter of time until you discover this the hard way)

No Waiting, No Reboots

Eliminate downtime

Installs patches to live (or staging) servers without performance impact or downtime.

Never miss a critical patch

Super-fast, latest security patch release – the agent checks for new patches every 4 hours.

Single-line rebootless installation

A few minutes to install, nanoseconds to update, with roll-back capability, all without reboots.

"The downtime that reboots cause is a disruption for customers, and nuisance for admins, that can be easily avoided with KernelCare. We're moving closer to a time in which this type of "disruption is no longer excusable."

JOE OESTERLING, Chief Technology Officer at Liquid Web

KernelCare Streamlines Costs

Avoid security issues

No more vulnerabilities as kernels are always up to date on all security updates.

Lower operating cost for server management

Automated patching frees up your IT team. No more middle-of-the-night & weekend maintenance windows.

We monitor security lists so your Admins don't have to.

No more application downtime for business users

Avoid application downtime due to kernel updates, eliminate the need to coordinate between various locations, users and Admins.

Cost Considerations with Traditional Kernel Updates

Operational Costs: *Due to maintenance windows and admin costs, timely updates and server reboots are difficult. Factors to consider:*

- Number of servers that need to be updated;
- % of servers that will have restart issues during a reboot;
- Damage control from issues arising within the timeframe of discovered vulnerability and a fix;
- Being non-compliant due to running unpatched software prior to next maintenance window;
- Number of Admins needed to perform updates;
- Days/hours spent by Admins performing repetitive maintenance, planning and updates, as opposed to more strategic IT initiatives.

Business Costs: *Various business units are affected by the downtime during the update. Factors to consider:*

- Business and opportunity cost of application downtime;
- Stakeholders involved in downtime planning;
- Risk factors related to security issues if they arise.

KernelCare

Using KernelCare

Admin costs related to:

One-time:
...KernelCare rebootless installation on each server.

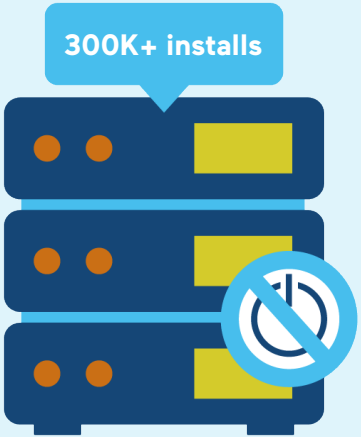
In rare cases... testing of patches on the staging environment.

KernelCare

Very Affordable Insurance

1 LICENSE	2-49 LICENSES	50-499 LICENSES	500+ LICENSES
$3.95	$2.95	$2.55	$2.25
per server per month	per server per month	per server per month	per server per month
$45 per server per year	**$33 per server per year**	**$28 per server per year**	**$25 per server per year**

1500+ companies, including Dell, Endurance, and LiquidWeb keep their Linux servers on and secure with KernelCare.



Supports Most Popular Linux Distributions

KernelCare supports automatic updates or managed updates in a live environment, or in your desired staging environment. Works on typical servers as well as virtual environments.

Amazon Linux 1 & 2 | CentOS/RHEL/CloudLinux OS 6 & 7 | CentOS Plus 6 & 7 | Oracle Linux RHEL-compatible 6 & 7, UEK 3 & UEK 6 R3 | Debian 7, 8 & 9 | Ubuntu LTS 14.04, 16.04 & 18.04 | OpenVZ & Virtuozzo | Proxmox VE 3, 4 & 5 | Xen4CentOS 6 & 7 | ...and more | *Custom kernel patching available*

aws CentOS redhat CloudLinux OS debian ORACLE LINUX ubuntu

The ONLY Live Kernel Patching Endorsed by AWS

How KernelCare Works

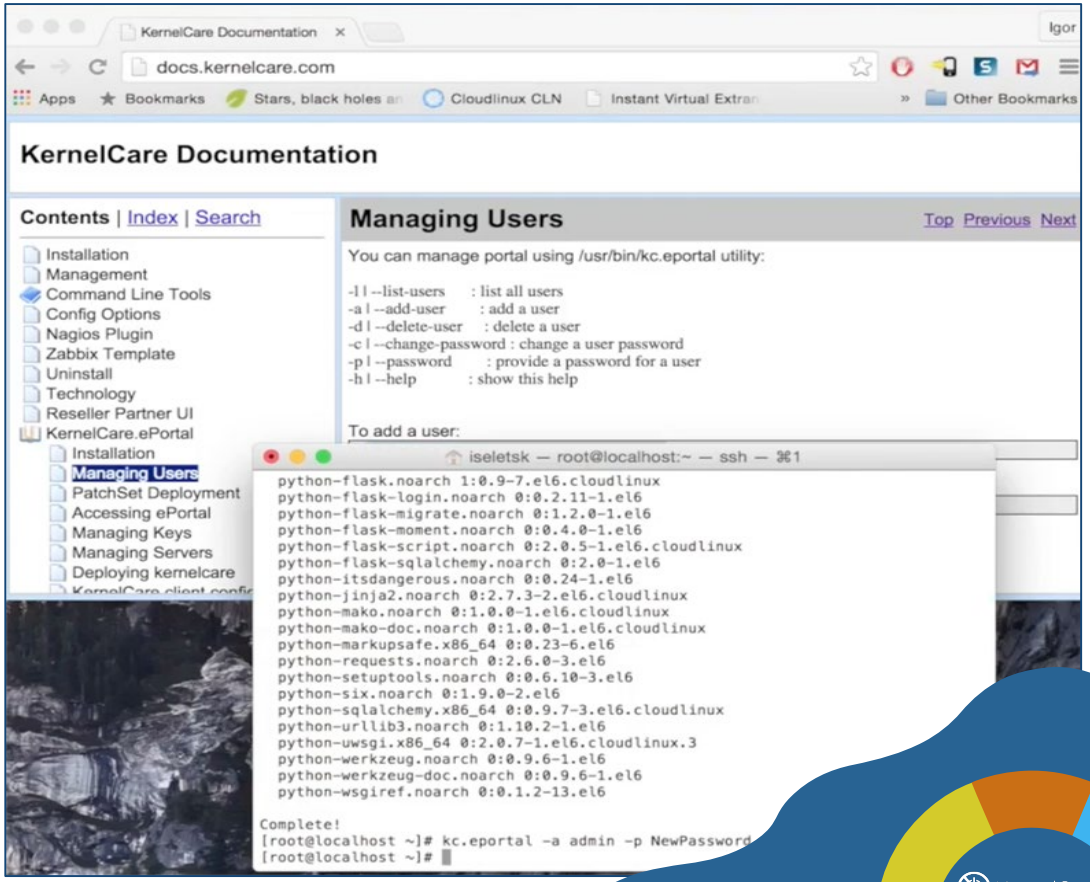
- Our security experts, with a deep knowledge of kernel development, monitor all Linux security lists 24x7x365;
- Once they notice a vulnerability that affects the supported kernel, they promptly prepare a security patch;
- Patch is compiled in a binary format and is deployed to KernelCare distribution servers;
- KernelCare agent checks for new patches every 4 hours and if any found, it downloads it and updates kernels without the reboot.

Protection against serious vulnerabilities such as DirtyCow, Meltdown and Spectre.

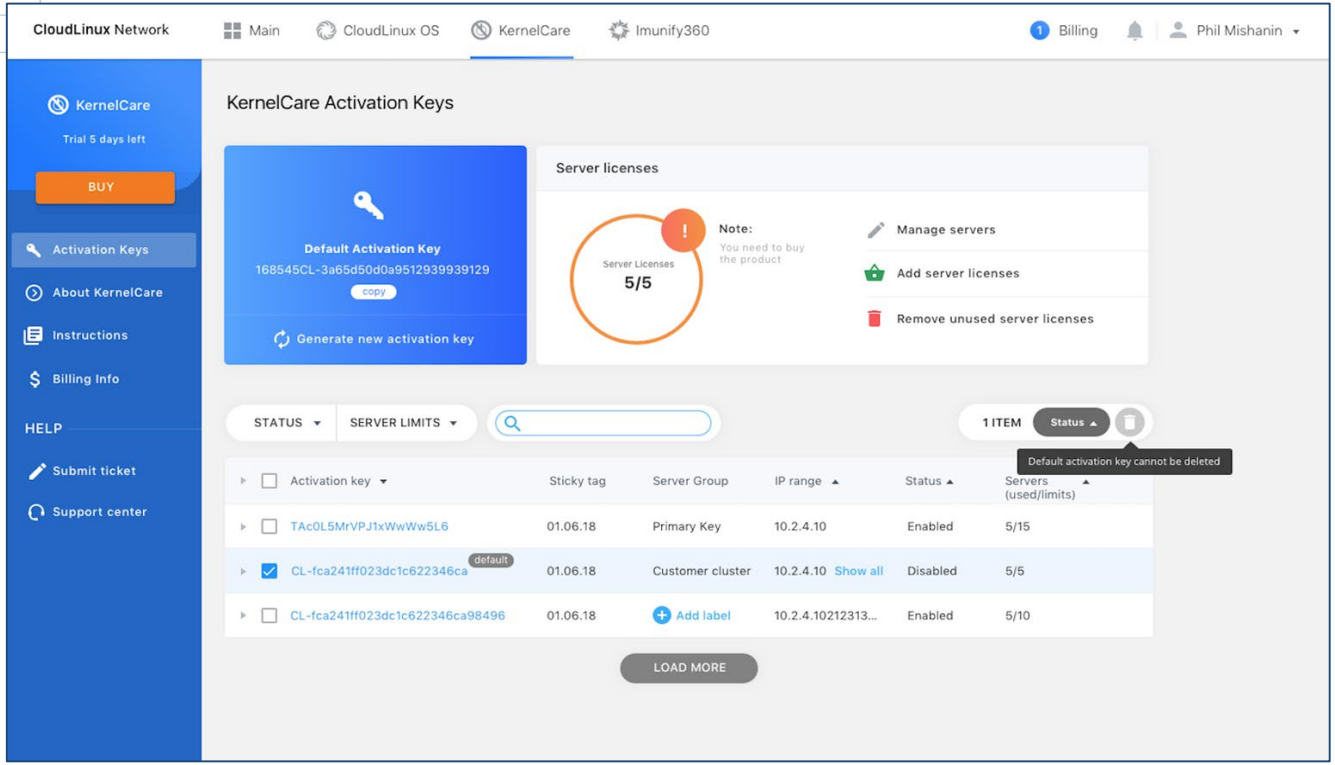
Built For The Enterprise

KernelCare.ePortal, an enterprise tool for security, control, and flexibility, allows Admins to manage patches for servers located behind the firewall or without an internet connection.

More information on KernelCare.ePortal can be found at **cloudlinux.com/kernelcare-eportal**



KernelCare



CloudLinux Network

KernelCare activation keys are managed via the intuitive interface.

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**.