



# 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.

# 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.


# Using KernelCare

Admin costs related to:

**One-time:**

...KernelCare rebootless installation on each server.

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



# Very **Affordable** Insurance

1 LICENSE

**\$3.95**

per server per month

\$45 per server per year

2-49 LICENSES

**\$2.95**

per server per month

\$33 per server per year

50-499 LICENSES

**\$2.55**

per server per month

\$28 per server per year

500+ LICENSES

**\$2.25**

per server per month

\$25 per server per year



# 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*

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

300K+ installs



The **ONLY** Live  
Kernel Patching  
Endorsed by **AWS**



Advanced  
Technology  
Partner

# 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.**





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](https://cloudlinux.com/kernelcare-eportal)

# Built For The Enterprise

The screenshot shows the KernelCare Documentation website in a browser window. The page title is "KernelCare Documentation" and the URL is "docs.kernelcare.com". The navigation menu includes "Contents", "Index", and "Search". The main content area is titled "Managing Users" and contains the following text:

You can manage portal using /usr/bin/kc.eportal utility:

```
-l --list-users : list all users
-a --add-user : add a user
-d --delete-user : delete a user
-c --change-password : change a user password
-p --password : provide a password for a user
-h --help : show this help
```

To add a user:

```
python-flask.noarch 1:0.9-7.el6.cloudlinux
python-flask-login.noarch 0:0.2.11-1.el6
python-flask-migrate.noarch 0:1.2.0-1.el6
python-flask-moment.noarch 0:0.4.0-1.el6
python-flask-script.noarch 0:2.0.5-1.el6.cloudlinux
python-flask-sqlalchemy.noarch 0:2.0-1.el6
python-itsdangerous.noarch 0:0.24-1.el6
python-jinja2.noarch 0:2.7.3-2.el6.cloudlinux
python-mako.noarch 0:1.0.0-1.el6.cloudlinux
python-mako-doc.noarch 0:1.0.0-1.el6.cloudlinux
python-markupsafe.x86_64 0:0.23-6.el6
python-requests.noarch 0:2.6.0-3.el6
python-setuptools.noarch 0:0.6.10-3.el6
python-six.noarch 0:1.9.0-2.el6
python-sqlalchemy.x86_64 0:0.9.7-3.el6.cloudlinux
python-urllib3.noarch 0:1.10.2-1.el6
python-uwsgi.x86_64 0:2.0.7-1.el6.cloudlinux.3
python-werkzeug.noarch 0:0.9.6-1.el6
python-werkzeug-doc.noarch 0:0.9.6-1.el6
python-wsgiref.noarch 0:0.1.2-13.el6
```

Complete!

```
[root@localhost ~]# kc.eportal -a admin -p NewPassword
[root@localhost ~]#
```

CloudLinux Network Main CloudLinux OS KernelCare Imunify360 Billing Phil Mishanin

### KernelCare Activation Keys

**Default Activation Key**  
168545CL-3a65d50d0a9512939939129

Generate new activation key

**Server licenses**

Server Licenses 5/5

Note: You need to buy the product

- Manage servers
- Add server licenses
- Remove unused server licenses

1 ITEM Status

Activation key	Sticky tag	Server Group	IP range	Status	Servers (used/limits)
<input type="checkbox"/> TAc0L5MrVPJ1xWwWw5L6	01.06.18	Primary Key	10.2.4.10	Enabled	5/15
<input checked="" type="checkbox"/> CL-fca241ff023dc1c622346ca <small>default</small>	01.06.18	Customer cluster	10.2.4.10 <a href="#">Show all</a>	Disabled	5/5
<input type="checkbox"/> CL-fca241ff023dc1c622346ca98496	01.06.18	<a href="#">+ Add label</a>	10.2.4.10212313...	Enabled	5/10

LOAD MORE

Default activation key cannot be deleted

# CloudLinux Network

KernelCare activation keys are managed via the intuitive interface.

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

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

**300K+**  
servers running securely  
without reboots with  
KernelCare