KernelCare

Deployment Guide for the Enterprise

How to integrate KernelCare into the enterprise environment.

KernelCare

Rebooting Your Servers is Making You Insecure and Noncompliant.

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

KernelCare applies security patches automatically to a running kernel. Live installation of security patches takes nanoseconds, doesn't alter the performance of servers, doesn't require a reboot, and quickly delivers a better, more secure Linux.

Enterprise Environment

A lot of servers don't have access to the internet and cannot install software from 3rd party repositories. KernelCare works by installing an agent on each server, that will download and install patches for the running kernel.

In a typical enterprise environment, the enterprise would:

1. **Install a new server with KernelCare.ePortal.** That server will need some access to the internet to download patches.
   a. Hardware requirements: https://docs.kernelcare.com/kernelcare_enterprise/#eportal-hardware-requirements
   b. Installation instructions: https://docs.kernelcare.com/kernelcare_enterprise/#installation
      - Video on how to install it: https://www.youtube.com/watch?v=E8QYy6LIR0E
   c. Connecting ePortal to patch server: https://docs.kernelcare.com/kernelcare_enterprise/#patchset-deployment
2. **Download/setup local repository for KernelCare agent** (kernelcare.rpm, kernelcare.deb packages).
   a. A mirror of this repository can be created internally: https://repo.cloudlinux.com/kernelcare (RPM BASED) https://repo.cloudlinux.com/kernelcare-debian/ (DEB BASED)
      - This script can be modified to use your local copy of the repo: https://kernelcare.com/installer
   b. Alternatively, individual RPM & DEB packages can be downloaded & used installed.

3. **Use puppet/chef/ansible or similar automation solutions to deploy the KernelCare agent on each server by running the installer, or by installing the individual package.**

   a. Setup PATCH_SERVER/REGISTRATION_URL to point to ePortal and disable automated updates
   https://docs.kernelcare.com/kernelcare_enterprise/#kernelcare-client-config-file

   b. Register server with `$ kcarectl --register _YOUR_KEY_`

      - See section on managing keys:
      https://docs.kernelcare.com/kernelcare_enterprise/#managing-keys

4. **When new patches are available, test them in staging environment, and after testing push them to production using puppet/chef/ansible or similar automation tools by running the command:**

   ```
   $ kcarectl --update
   ```

Overall Architecture

Note: only ePortal will have access to our patch server. It will connect to HTTPS port 443 of the Patch server. Patch server doesn't have a way to connect to ePortal server.

Single Sign-On integration

KernelCare supports LDAP for SSO. Other SSO providers can be added on demand
https://docs.kernelcare.com/kernelcare_enterprise/#ldap-authorization

ePortal.API

https://docs.kernelcare.com/kernelcare_enterprise/#eportal-api
KernelCare.ePortal provides limited API to remove servers based on key & IP.

To access the API, first setup API token used for authentication:
echo your_token > /usr/share/kcare-eportal/config/api.token
API method: unregister_by_key.plain

Parameters:

- key - KernelCare.ePortal key under which server is registered;
- IP - remote server IP as displayed in KernelCare.ePortal;
- token - API token.

Example:

https://ePortal_url/admin/api/kcare/unregister_by_key.plain?key=2M6gmIS6fHh39aF2&ip=10.1.10.74 &token=your_token

Return code: int

- -3 - API token file does not exist;
- -2 - API token doesn't match;
- -1 - Internal error, see /var/log/uwsgi/uwsgi-emperor.log for details;
- any other number - number of servers removed.

API to integrate with the monitoring system

KernelCare integrates with Nagios & Zabbix
https://docs.kernelcare.com/kernelcare_enterprise/#nagios-zabbix-support
Yet, integration with other systems by connecting to:
https://ePortal/api/kcare/nagios/
Given a key, it will return the status of each server (if it is updated, not updated, etc...)

Integration with scanning vendors

KernelCare patches kernel in-memory, without changing RPM on disk or reported kernel version in /proc/version. As a result, most scanning vendors will not identify that kernel was patched. KernelCare has integration with Rapid7 solution to correctly mark patched vulnerabilities in the report as 'exception', by correlating patches installed on each server with the report.
https://docs.kernelcare.com/kcare-nexpose/
Other scanning vendors can be added on demand. We have also helped companies integrate with their in-house scanning tools.

Source Code

KernelCare ships patches in binary format, yet we do provide our patches in source code format (under NDA) to interested parties

KernelCare

Technical FAQ

Where do I go for documentation or support?

You can contact our support at helpdesk@kernelcare.com. You can find KernelCare documentation at docs.kernelcare.com.

Can I use a single KernelCare key to register multiple servers?

Yes. The KernelCare key can be used to deploy and register multiple servers at once. Visit this page to learn more.

Can KernelCare run on servers that don't have access to the internet?

Yes. KernelCare can run on servers located behind the firewall using KernelCare.ePortal. To learn more how KernelCare.ePortal works, view this video.

Do I need to reboot my server after I installed KernelCare?

There is no need to reboot the server after KernelCare installation.

Which kernels does KernelCare support?

Visit this page for a list of supported kernels. You can also find patches available for each kernel here. If you are running an unsupported distribution or your kernel is custom, self-compiled, special, we provide a custom kernel patching service.

How can I check if my kernel is supported by KernelCare?

Visit this page to learn how to check whether your kernel is supported.

Where can I signup to receive information about new KernelCare patches?

You can signup for mailing lists here.

What happens if I install KernelCare but my kernel is not supported?

If your kernel is not supported, KernelCare will detect it and will do nothing. There is no danger (but also no benefit) of running KernelCare on unsupported kernels. KernelCare will provide a message "Unsupported Kernel" when it doesn't know anything about a particular kernel. See the list of supported kernels or learn how to check whether your kernel is supported.

Should I continue updating my OS as before?

Yes. KernelCare will provide important updates for your kernel, but you still need to continue to update your userland applications.

Will KernelCare work with 3rd party drivers?

Yes, KernelCare will work with 3rd party drivers. The driver itself will not be updated.

How can I check if I am running latest updates?

Execute as root: */usr/bin/*kcarectl *–info d*

How to uninstall KernelCare?

Execute as root: *yum remove* kernelcare

How can I disable automatic updates?

Edit file */etc/*sysconfig/kcare/kcare.*conf*
Set *AUTO_UPDATE=False*

How can I see the 'updated' version of the kernel?

Run: */usr/bin/*kcarectl --uname
For your convenience, we provide this script */usr/bin/*kcare–uname that has the same syntax as uname

How can I see which patches were applied to my kernel?

Execute as root: */usr/bin/*kcarectl *–patch-info*

Is KernelCare software released under open source?

The kernel module is released under GPL2, and you can download it here: http://patches.kernelcare.com/kmod_kcare.tar.gz.
Other components are distributed in binary-only format under the KernelCare License.

Who develops KernelCare patches?

Patch creation requires a strong background in kernel development as well as a powerful toolset to prepare and test the patches. The KernelCare team consists of a group of highly qualified kernel developers working full time on just monitoring security and kernel mailing lists and preparing the patches.

Are you using the same technology as the one from Oracle, Red Hat or Suse?

No. Our technology was fully developed in-house and uses different methods to generate the patches as well as to apply them. We believe that our method of generating patches is significantly more efficient than what we have seen or read up to date from other vendors.

How to migrate from Ksplice?

Click here to learn how to migrate to KernelCare from Ksplice.

Do you apply all the patches from the newest kernels?

We apply only security patches. Sometimes we might decide to apply patches for critical bugs as well.

Can patches crash the server? And will server keep crashing on reboot?

That is highly unlikely, as we test patches internally, and then make it available on 100K+ servers before they are pushed to enterprise clients.
We never had a problem with a patch repeatedly crashing a server. Also, such condition is completely impossible on a server with automated updates off, as kernel patches will not load automatically on reboot.

How can I make kernel patches to load automatically on reboot?

Either enable automated updates or add:
kcarectl --update in rc.local or similar script that executes after reboot.

How can I uninstall patches:

Execute:
$ kernelcare --unload

Do I need to do something when I boot in a new kernel?

No action is needed in such a case. KernelCare will automatically figure out which kernel is running and will download the right set of patches when kcarectl --update gets executed

KernelCare Whitepapers

Technical whitepaper:

https://www.kernelcare.com/wp-content/uploads/2019/04/KernelCare-Technical-White- Paper.pdf

Compliance/KernelCare whitepaper:

https://cdn2.hubspot.net/hubfs/5408110/Kernelcare%20-%20Whitepaper.pdf