KernelCare and Ivanti patch management solutions

Automated Linux kernel security updates without reboots

KernelCare

ivanti ONE CERTIFIED

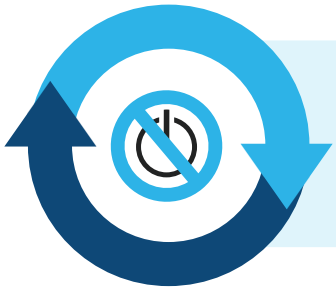
KernelCare

KernelCare for Ivanti

Automated Linux kernel security updates without reboots

Rebooting your servers is making you insecure and incompliant

The kernel is the most important part of any Linux system. It provides vital low-level functions to the entire system. Any security issues detected within it jeopardize the whole server. Kernel patching is a background activity, carried out by System Administrators without too much fuss. It is generally ignored altogether by those responsible for security and compliance. However, this is a dangerous oversight. The standard approach to kernel patching exposes servers to malicious intent by threat actors on multiple attack vectors, putting IT organizations at risk of major security issues. Anyone tasked with keeping their organization safe should be seeking a better way.



KernelCare patches Linux systems while they are operational

KernelCare is patch management software that automatically keeps Linux kernels up to date with the latest security patches. No server rebooting or system downtime is necessary. It is fast, simple and easy to deploy, and can deliver complex patch configurations without affecting performance or stability. It is available for all major Linux distributions.

Amazon Linux **1 & 2**	CentOS **6, 6 Plus, 7, 7 Plus**	CloudLinux OS **6, 6 Hybrid, 7 & 8**	RHEL **6, 7, 8**	Debian **7, 8, 9**	Ubuntu **14.04, 16.04, 18.04, 20.04**
Xen4CentOS **6, 7**	Proxmox VE **3, 4, 5**	Proxmox **6**	Oracle Linux **UEK 3, UEK 4, UEK 6, UEK 6 R3**	Oracle Linux RHEL **- Compatible 6, 7**	Embedded Distros: **Yocto, Ubuntu Core**

At **KernelCare**, our kernel development team monitors security mailing lists. When a vulnerability affecting supported kernels is announced, we prepare a patch as soon as technically possible.

A **KernelCare** agent process running on your server synchronizes and checks with our distribution servers every four hours (or an interval you configure).

We compile each patch for that kernel and deploy it to our distribution servers.

When a new patch is available for the active kernel, the agent downloads it and applies it to the running kernel in memory:

- NO need to reboot
- NO service interruptions or packet drops
- NO need to kill any processes or user sessions.

With KernelCare, there is no need to wait for the next maintenance window or reboot cycle. Kernel security updates are applied as quickly as possible, typically within one or two days of CVE public announcement.

We have come to consider KernelCare as an essential service. The downtime that reboots cause is a disruption for customers, and nuisance for admins, that can be easily avoided with KernelCare."

Joe Oesterling, Chief Technology Officer at LIQUID WEB

KernelCare Technical Overview

KernelCare runs as a service that live-patches a running Linux kernel. A small agent installed on a server applies binary kernel patches. These are downloaded directly from the main KernelCare Patch Server which can be accessed directly or through a firewall (via a proxy server), or a local private patch update server (KernelCare ePortal) can be self-hosted to synchronize and deliver the patches.

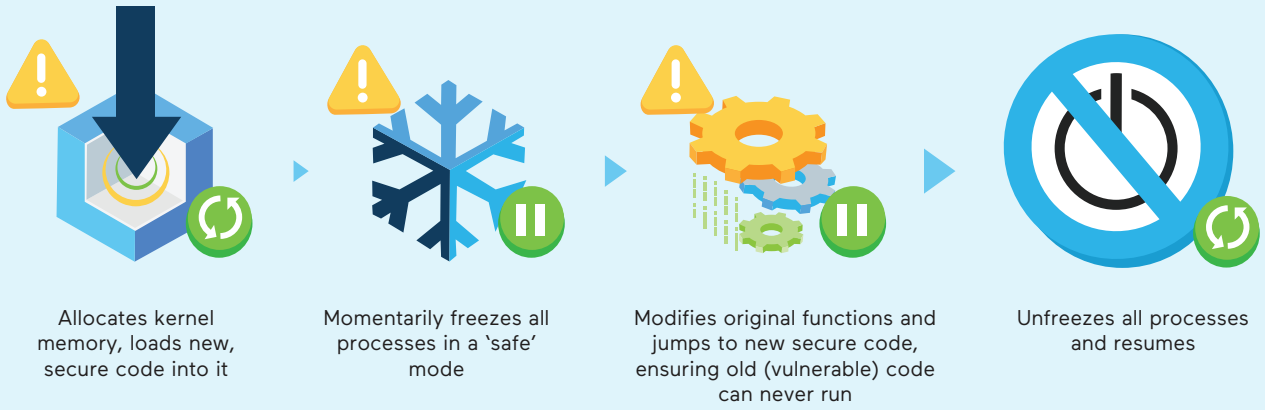


Figure 1: KernelCare patching process diagram

Patches are distributed as atomic binary packages, custom-built for each supported kernel version, and each is encrypted and signed with a GPG (GNU Privacy Guard) key for security. This method allows our patches to be persistent since new patches are all-encompassing and not simply 'stacked' on top of old patches. All patch updates are fully auditable and can be selectively pre-tested, approved, or abandoned and rolled back with a single command.

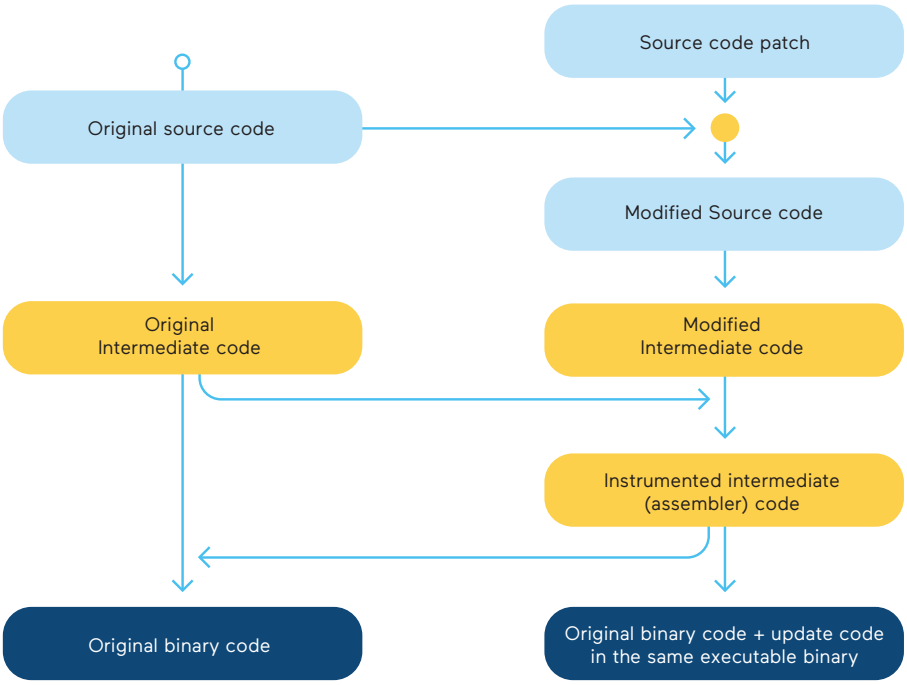


Figure 2: KernelCare architecture view

Ivanti Patch Management Solutions Key Benefits

Ivanti Security Controls

Ivanti Security Controls simplifies security with a unified solution that creates the highest barriers to modern cyber-attacks. This solution includes discovery of authorized and unauthorized software; patch management for heterogeneous OS and third-party app environment; dynamic whitelisting; and granular privilege management—as well as additional patch tools that help IT and Security work together to protect the business.

Features

Single automated patching solution: patch for Windows and Linux solution spans physical and virtual Windows servers as well as workstations. Also includes non-Windows OSes such as Red Hat Enterprise Linux and CentOS patch support.

Dynamic whitelisting and privilege management: option in place using trust models that reduce ramp-up, lower cost of ownership, and increase performance while still delivering a high degree of security. This also lets IT take back admin rights controls without needing to ease additional permissions.

Additional patch tools to secure organizations: makes life easier for Security and IT Ops teams. Patch REST APIs enable integration with other products, automate shared processes, and provide remote access and control of the console. CVE to patch list creation takes a vulnerability assessment from vendors an organization is using, finds all the patches that relate to these CVEs, and builds a patch group of updates that can be quickly approved for remediation.

Ivanti Patch for Endpoint Manager

Patch for Endpoint Manager simplifies how to get things finished with the ability to secure and manage from a single console. With Ivanti Patch for Endpoint Manager, enterprises can consistently discover, assess, and remediate thousands of client systems based on defined policies without saturating networks or disrupting user productivity.

Features

Pain-free, comprehensive patching: displays patches installed on all client systems, including patches installed from Ivanti software or others. Performs vulnerability assessment using industry-standard sources from the largest patch catalog to remediate thousands of third-party application vulnerabilities for Windows and Mac.

Protect your bottom line with greater compliance: helps organizations meet compliance requirements and regulatory standards reducing the risk of legal and financial penalties. Swiftly detects vulnerabilities in Windows, Mac OS, Linux, and hundreds of third-party apps and deploys expertly pre-tested patches.

Patch faster and reduce network impacts: distributes and deploys patches quickly without creating expensive bandwidth demands. Organizations can control when patches are installed and whether to reboot or snooze selected systems after patching.

What is unique about the collaboration between KernelCare and Ivanti?

KernelCare

ivanti ONE CERTIFIED

Ivanti provides proven, industry-leading patch management solutions that keep critical operating systems and third-party apps up to date. However, enterprises today industry-wide cannot securely patch Linux kernels without restarting Operating Systems.

KernelCare solves Linux system interruption challenges by eliminating security patch reboot cycles and maintenance schedules without shutting them down. Used together, Ivanti and KernelCare services form an enterprise security framework that helps organizations improve uptime and reduce service disruptions from their Linux servers and workstations.

Install KernelCare on all your Linux instances to try free for 30 days:

TRY NOW

Download KernelCare from Ivanti Marketplace:

DOWNLOAD NOW