Datasheet

TuxCare

# How to Avoid 12 Disruptive Reboots (or More) per Year

In conventional patch management, SysAdmins need to schedule a system reboot to apply Linux kernel patches.

**The processes required to perform these inconvenient reboots involve a number of challenges:**

IT teams usually need to deal with **chaotic coordination across multiple departments** to align reboot timing.

Team members must **babysit hours-long reboots** (usually during off-hours like nights and weekends).

**Services are interrupted or degraded** while the reboot is happening, which end-users often become aware of.

Sales opportunities, account renewals, and potential partnerships are put at risk as **stakeholders take notice of the disruptions** involved.

Waiting for a time slot when a reboot can be performed **leaves systems vulnerable to cyber attacks** for a longer-than-needed window of time.

> **Our clients rely on the availability and reliability of our services, and any disruptions or downtime can have severe repercussions for their business operations, reputation, and, ultimately, bottom line.**
>
> - Principal Engineer of Cloud Architecture at Proofpoint

Read the Customer Story

> **The kernel patches needed to fix vulnerabilities were a burden to the system administration staff, in part because it brought unwanted downtime.**
>
> - System Engineer at the University of Zagreb

Read the Customer Story

These reboots aren't only inconvenient and potentially damaging – they're frequent.
**In many industries, organizations perform these reboots approximately once per month – leading to 12 disruptive system restarts per year.**

**That means:**

### 12 disruptions to services/business operations

Critical applications and services are temporarily unavailable.

### 12 interruptions of processes and data transfers

IT teams must shift focus to manage the reboot process.

### 12 off-hours shifts

IT team members often need to babysit reboots during nights and weekends.

### 12 dips in productivity

Teams need to coordinate and schedule maintenance windows.

### 12 user experience degradations

Customers may face degraded service or temporary outages.

### 12 data synchronization delays

Processes and data transfers may be interrupted or paused.

**...and, even then, this approach doesn't respond fast enough to new threats.**

# Fortunately, there's a way to avoid ALL of this – with Rebootless Patching from TuxCare.

## KernelCare Enterprise from TuxCare

Deploy all the latest vulnerability patches, automatically, in the background while your Linux systems are running, so you can stay patched with:

- Zero Reboots
- Zero Downtime
- Zero Headaches

**But KernelCare is more than just a tool that takes reboots and downtime out of your patching processes. It also enables your organization to:**

### Eliminate Maintenance Windows

Leave the chaos of coordinating patching-related maintenance windows behind and regain control over your schedule.

### Streamline Security Compliance

Ensure continuous compliance with tightening regulatory requirements and various cybersecurity standards.

### Minimize Vulnerability Risk

Apply kernel security updates as soon as they become available and win the race against vulnerability exploits.

### Cut Operational Costs

Achieve major cost savings by eliminating downtime and removing the hassle of managing system reboots.

## Get started with a free 30-day demo at www.tuxcare.com

### Certifications

FIPS VALIDATED 140-1 140-2

AICPA SOC

PCI DSS LEVEL 1 SERVICE PROVIDER

EU GDPR COMPLIANT

CCPA

SAM SYSTEM FOR AWARD MANAGEMENT

### Awards

2021 GLOBEE AWARDS GOLD WINNER IT WORLD AWARDS INFORMATION TECHNOLOGY CYBER SECURITY

BRONZE 2023 STEVIE WINNER AMERICAN BUSINESS AWARDS

CYBER SECURITY EXCELLENCE AWARDS WINNER 2023

GOLD 2022 STEVIE WINNER INTERNATIONAL BUSINESS AWARDS

MERIT AWARDS Information Security TuxCare GOLD

BRONZE 2023 STEVIE WINNER FOR SALES & CUSTOMER SERVICE

### Follow TuxCare on Social Media

☎ +1 (800) 231-7307 ✉ sales@tuxcare.com