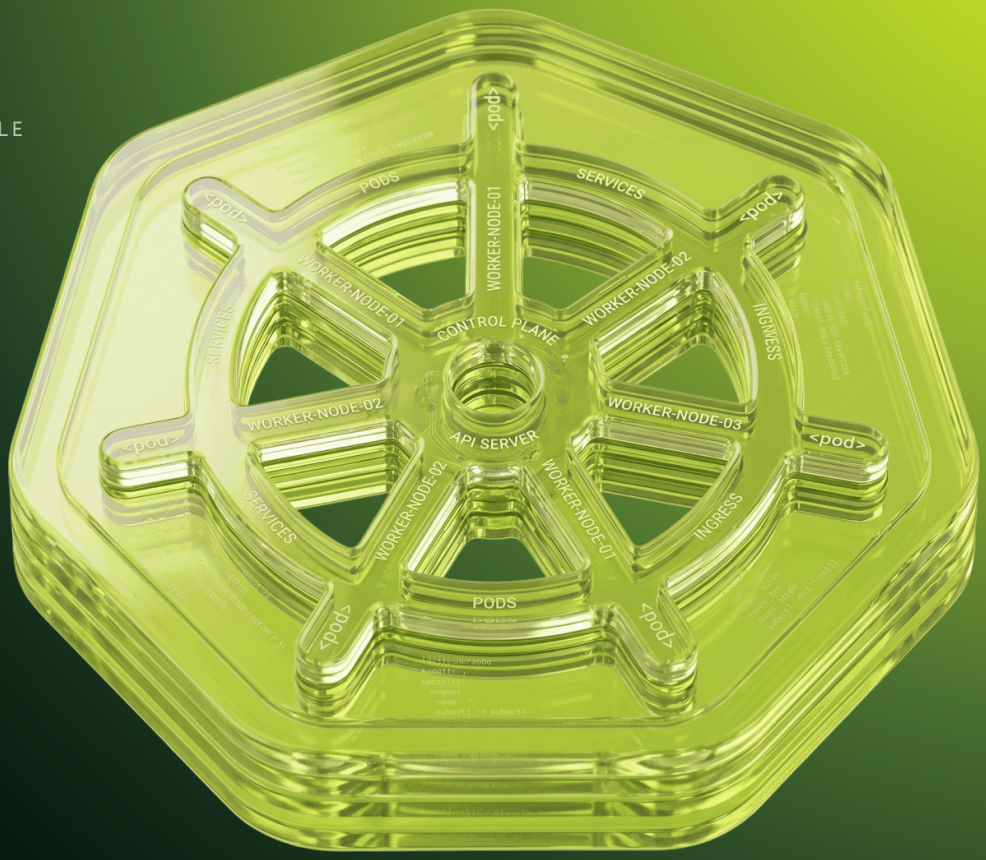
OPSWERKS CASE STUDY

PLATFORM RELIABILITY AT SCALE



Over 5,000 EKS Nodes Patched in Less Than a Week to Prevent Attacks

How a Fortune 100 platform team patched a critical Kubernetes vulnerability across its fleet in days, not the standard month.

5,000+
EKS nodes patched in under a week

Under 7 days
compressed from a 30-day compliance cycle

Zero
P0/P1 incidents caused by the rollout

The Challenge

When a critical vulnerability drops, can you patch your entire Kubernetes fleet in days, across every team, without taking down production? For one Fortune 100 technology company, that question became real.

The affected infrastructure provides the foundation for business-critical services used by hundreds of millions of customers worldwide.

With exploit code public and active, the pressure on the platform team left no margin for error: apply the patch quickly, without any service disruption.

The standard remediation window is 30 days. Given the severity of the vulnerability, management requested the fleet be patched that week.

About the vulnerability

- Critical Linux kernel flaw: Severe enough to require immediate remediation rather than a scheduled patch cycle.
- Full root escalation: Any logged-in user could secretly rewrite protected system files and escalate to root on the underlying node.
- Deterministic and silent: The exploit ran reliably and left no trace on disk.
- Publicly exploited: Working exploit code was already circulating and in active use.

OpsWerks was already inside the fleet

OpsWerks regularly runs planned EKS upgrades and ongoing vulnerability remediation across this fleet. The engineers who responded are the same ones who operate it day to day, so there was no ramp-up and no relearning a system from scratch.

No ramp-up

The responding engineers operate this fleet every day. No onboarding, no discovery phase, no waiting for resources to be assigned before work could start.

Known approval paths

Familiarity with the environment, the approval paths, and the OpsWerks-built tooling is what made an accelerated response possible at all.

Prior upgrades at this scale

Large-scale EKS upgrade experience let the team take on 5,000+ nodes across multiple locations on a very compressed timeline.

- Certified Kubernetes Administrator (CKA)

- Certified Kubernetes Application Developer (CKAD)
- AWS Certified Solutions Architect - Associate
- AWS Certified Cloud Practitioner

The OpsWerks approach

OpsWerks delivered the entire accelerated response inside the existing engagement, compressing a 30-day remediation window to under a week. No SOW amendment. No change order tickets. No added cost.

End-to-end ownership

OpsWerks owned coordination, communications, approvals, pre-checks, execution, monitoring, and post-checks. The customer's FTE manager set cluster sequence and patching priority.

Phased rollout to minimize risk

Lower environments first (dev, qa, perf), then cert, staging, and production. US East and US West ran on separate days.

Proven tooling

Deployment ran on OpsWerks-built scripts, with every batch validated by pre-check and post-check health scripts.

Live monitoring at high-risk windows

Grafana and Prometheus dashboards, tuned across prior engagements, tracked every batch. Manual watch during high-risk windows let the team act before alerts fired.

Coordination and approvals

Open conference calls and dedicated Slack threads, grouped by team owner, kept teams aligned. OpsWerks managed approvals, escalating delays through the FTE project manager.

Days, not a month

A 30-day compliance cycle closed in under seven, absorbed inside the existing engagement with no change orders.

The catch that saved regional failover

An OpsWerks engineer caught that the customer's traffic engineering stacks were running a different EKS version that had to be upgraded first. If the sequence had been wrong, regional traffic failover would have broken at cutover, on services used by hundreds of millions of users. The team raised it, replanned, and executed without disruption.

Saying nothing would have been easier, and a failure at cutover would only have meant more work for OpsWerks. The team raised it because it was right for the customer.

Results

EKS NODES PATCHED IN UNDER A WEEK

5,000+

COMPRESSED FROM A 30-DAY COMPLIANCE CYCLE

Under 7 days

P0/P1 INCIDENTS CAUSED BY THE ROLLOUT

Zero

DELIVERED INSIDE THE EXISTING SOW

No added cost

Impact

Without OpsWerks, the nodes serving hundreds of millions of customers would have been exposed to a public, actively exploited vulnerability for potentially up to a month.

With OpsWerks, the response started immediately: no delayed kickoff, no waiting for resources to be assigned. The exposure window closed in under a week, the failover risk was caught and removed before rollout, and zero P0 or P1 incidents touched production.

OpsWerks absorbed the accelerated request inside the existing engagement, so the customer's cloud engineering, traffic engineering, and application teams kept focus on their roadmaps instead of dropping everything to firefight. This is outcome ownership in practice: OpsWerks is measured by problems removed, not by hours billed or tickets left open.

> "Thanks a lot for the amazing work this week. It was no easy feat to patch over 5,000 nodes within a week. Thank you for coming together as a team to make this happen on such short notice and within such a short time frame. Really appreciate it."
>
> CLOUD ENGINEERING LEADER, FORTUNE 100 TECHNOLOGY COMPANY

Facing similar challenges?

Talk with the team that delivered this work. We will map your environment, your constraints, and what OpsWerks would own.

Schedule a discovery call

PARTNERWITHUS@OPSWERKS.COM · OPSWERKS.COM