

OPSWERKS CASE STUDY

PLATFORM RELIABILITY AT SCALE



Securing and Stabilizing Critical Infrastructure for a Multinational Consumer **Electronics Firm**

Bringing 100,000+ hosts up to security standards: how OpsWerks automated critical maintenance, saving time and keeping innovation on track.

100%

of hosts up to security compliance

6 months

to reach full compliance

Edge cases

all that remain of dependency errors

Client Background

Our client, a multinational consumer electronics firm, relies on critical infrastructure of over 100,000 hosts that support development platforms and essential internal applications.

With mounting technical debt and the need to align with rigorous security standards, their SRE team faced a significant challenge in balancing maintenance with delivering strategic features.

The client chose OpsWerks to ensure all hosts remained secure and up to date without interrupting user services or missing internal SLAs and SLOs.

Challenges at 100,000-host scale

The client's SRE team was tasked with both introducing new services for internal development teams and handling the maintenance of the underlying hosts. This work created conflicting objectives, leaving little room for innovation.

Conflicting objectives

One team owned both new services for internal development teams and the upkeep of the hosts beneath them. Strategic delivery and routine maintenance competed for the same hours, and maintenance usually won.

Recurring maintenance load

Kernel patches, dependency updates, and Linux versioning had to be repeated across more than 100,000 hosts every cycle, against a backdrop of mounting technical debt and tightening security standards.

No room for disruption

Every host had to stay secure and current without interrupting user services or missing internal SLAs and SLOs. Maintenance windows offered no margin for error.

Solution for automating maintenance at scale

OpsWerks assumed full responsibility for security patching and maintenance, designing a layered automation framework that integrated with the client's existing tools without disruption.

Full ownership of patching

OpsWerks took responsibility for security patching and maintenance end to end, covering kernel patches, dependency updates, and Linux versioning.

Layered automation framework

Automation designed in layers and built to integrate with the client's existing tools rather than replace them.

Quarterly maintenance automation tool

A purpose-built tool that updates every host to the security standards specified by the client's security team, quarter after quarter.

Dedicated cross-functional team

A project manager, developers, and SREs working as one unit to keep a complex process fast, consistent, and reliable.

Existing monitoring, reused

By reusing the client's current monitoring infrastructure, the transition landed smoothly with minimal disruption.

Consistent feedback loop

Findings fed back to the client's teams each cycle, cutting repetitive toil instead of quietly absorbing it.

Scope of work

- Quarterly maintenance automation: Built a tool that brings each host up to the security standards defined by the client's security team.
- Security patching and maintenance: Kernel patches, dependency updates, and Linux versioning across 100,000+ hosts.
- Monitoring integration: Reused the client's current monitoring infrastructure for a smooth transition with minimal disruption.
- Dedicated delivery team: Project manager, developers, and SREs assigned to the engagement and trained once.
- Service continuity: Kept hosts secure and up to date without interrupting user services or missing internal SLAs and SLOs.

The OpsWerks advantage

One team, trained once

A dedicated, cross-functional team that trained once and operated without disruption, eliminating the need for retraining due to attrition, rotation, or sick coverage.

Outcome, not ticket counts

Unlike traditional vendors that optimize for ticket counts or task completion, OpsWerks aligned with the client's desired outcome: secure, uninterrupted infrastructure at scale.

Toil out, capacity back

By providing consistent feedback, OpsWerks reduced repetitive toil and enabled the client's SREs to refocus on delivering strategic platform capabilities.

Results

“

“I’ve been in this industry for almost 19 years. I’ve never seen a vendor that does such a great job of cross-training their teams and following through on the information given to them.”

INFRASTRUCTURE DEPLOYMENT AND HARDWARE SRE MANAGER

Results at a glance

OF HOSTS UP TO SECURITY
COMPLIANCE

100%

TO REACH FULL COMPLIANCE

6 months

ALL THAT REMAIN OF
DEPENDENCY ERRORS

Edge cases

SRE TEAM REFOCUSED ON
INNOVATION

Freed

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](https://opswerks.com)

