24/7 Incident Response Keeps Payments Flowing for Millions

OpsWerks resolves 85-90% of alerts at first contact, preventing escalations and ensuring reliability of a global payment ecosystem.

Client Background

A leading tech enterprise runs a payment ecosystem spanning digital wallets and tap-to-pay services used by hundreds of millions of consumers and businesses worldwide. Outages or moments of instability cause failed transactions, abandoned purchases, and surges in support calls.

In this environment where disruptions shake trust and drain revenue, DevOps and SRE teams carry the weight of ensuring reliability at massive scale 24/7. Their north star: resolving incidents before customers feel the impact.

Challenges for incident response

End users expect transactions to be instant. But just a 30-second delay in incident response raises the risk of degraded payment flows and processing errors. With so much at stake, DevOps and SRE teams wrestled with systemic challenges:

Alert noise

Up to 1,000+ alerts per month from Splunk, customer support, and internal tools overwhelm incident response teams, increasing mean time to detect (MTTD) and acknowledge (MTTA) payment incidents. Poorly tuned thresholds feed alert fatigue and complicated severity classification (P0/P1/P2), slowing triage.

Fragmented visibility

Incident data is scattered across multiple monitoring tools, support queues, API errors, and partner channels, including alerts, IM tickets, and emails. Without a unified view, frontline responders must manually correlate signals for every event, extending MTTD and MTTA.

Complex ecosystem

Payment services rely on the company's internal systems in addition to external systems run by banks, credit card companies, and integrators. For responders, this fragmentation makes it hard to isolate failures, engage the right owner, and keep everyone informed during outages.

Solution for transforming incident response

Internal SREs ran incident command but lacked a dedicated 24/7 frontline incident response (IR) team. To fill this mission-critical role, they chose OpsWerks, a trusted partner embedded with their team's tech stack, and runbooks.

While monitoring 24/7, the OpsWerks IR team tracks error counts, impact signals, and anomalies. This proactive approach, backed by rigor, drives rapid detection, acknowledgement, triage, and resolution. The improvements are measurable:

4–6x faster acknowledgement

OpsWerks has reduced MTTA from over one minute to 10–15 seconds. The team achieved this by developing custom notification tools integrated with PagerDuty and Slack, consolidating noisy alerts, filtering false positives, and expanding runbook automation for faster future resolution.

30–60% noise reduction

By fine-tuning Splunk/PagerDuty thresholds, consolidating duplicate alerts, and adding runbook-driven suppression, OpsWerks cuts false positives by 30–60%, shrinking noise and escalation fatigue. The team reviews "top polluters" weekly to keep parameters calibrated, ensuring responders focus on real incidents.

85–90% first-contact resolution (FCR)

The team resolves 85-90% of alerts without needing to escalate to internal teams. They use runbooks and automation — or resolve novel, first-time incidents based on their incident management expertise.

Unified dashboards optimize visibility

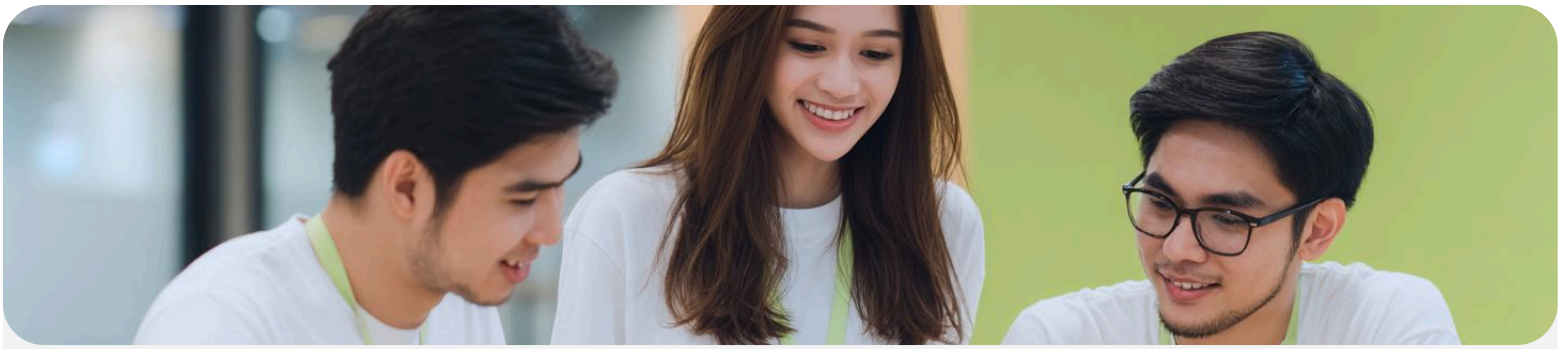
OpsWerks built and continually enhances custom Tableau dashboards that consolidate Splunk alerts, API errors, and support tickets into a single pane of glass. Internal teams can see incident data in one place, accelerating end-to-end incident response and coordination.

Partner communications

As a trusted extension of the company, OpsWerks acts as a liaison with banks, card networks, and integrators, informing partners of outages and recovery progress. By handling partner comms, OpsWerks enables internal SREs to focus on incident command until critical incidents are resolved.

Relentless post-incident improvements

Going well beyond frontline incident response, the OpsWerks team identifies recurring patterns, contributes to root cause analysis, updates runbooks, and drives follow-up actions to closure. Their continual efforts strengthen reliability over time.



Scope of work

- **24/7 frontline response:** Took ownership of incident detection, acknowledgement, triage, and first-contact resolution.
- **Noise reduction:** Consolidate and tune 1,000+ monthly alerts across Splunk, APIs, and support channels to filter false positives and prioritize true incidents.
- **Unified visibility:** Built dashboards giving teams a single view of incident data.
- **Third-party liaison:** Communicate outages and recovery progress with partners.
- **Post-incident improvements:** Provide RCA support, document patterns, update runbooks, and ensure follow-up actions are owned and completed.

The OpsWerks advantage

Outcome focus: Free internal SREs to lead incident command and long-term reliability initiatives while OpsWerks own the frontline.

Frontline continuity: Filled the client's missing 24/7 incident-response frontline with follow-the-sun coverage and seamless handoffs.

Proactive and automated: Enable early detection and resolution with custom notification tools, continuous monitoring, and automation across runbooks and workflows.

Embedded expertise: Long-standing integration with internal teams and deep familiarity with their tools and runbooks streamlined ramp-up and ongoing collaboration.

Results

Up to 90% first-contact resolution

Most alerts handled by OpsWerks with only high-severity incidents escalated to internal teams.

30–60% noise reduction

Fine-tuning alerts cut the number of false positives, enabling responders to focus on real incidents.

Unified visibility

Built Tableau dashboards to consolidate Splunk alerts, API errors, and tickets into a single pane of glass for responders and stakeholders.

4–6x faster acknowledgement

Reduced MTTA from just over a minute to 10–15 seconds with custom notification tools and streamlined workflows.

Facing Similar Challenges?

Contact our Partner Success Team at partnerwithus@opswerks.com to see how we can help.

About OpsWerks

- OpsWerks is a trusted partner to the world's most elite platform and infrastructure engineering teams, helping them operate at scale.
- We streamline hybrid cloud operations, execute complex migrations without downtime, and enable developers to quickly build and deploy global apps used by hundreds of millions.
- From managing CI/CD ecosystems and building orchestration tools to 24/7 support for business-critical systems, for over a decade we've kept developers focused on building.