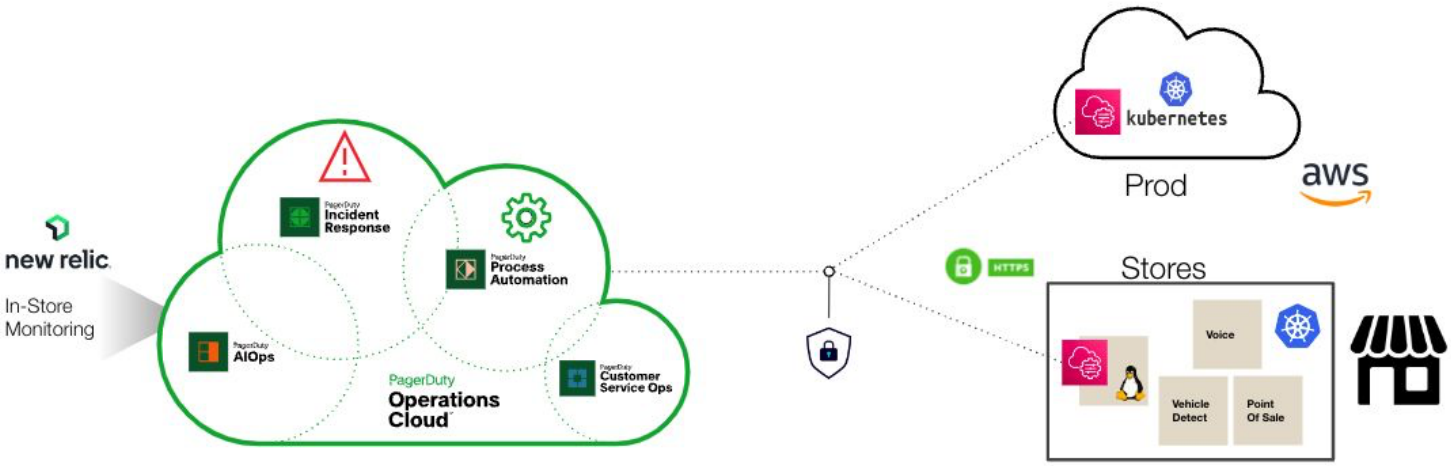
Use Case Brief:

Automating Edge Computing

PagerDuty

PagerDuty Operations Cloud helps you automate incident resolution and overall operations of your edge and IoT systems to maximize up time and efficiency. The Operations Cloud bridges team silos with automation that allows self-service and event-based coordinated workflows to happen without disrupting expert teams. This allows you to standardize remote IoT operations and delegate them for reuse as self-service, scheduled, and triggered requests.

Companies are deploying thousands of edge computing devices to bring digital transformation to their physical world customer experiences. Ensuring availability of these remote IoT systems places a burden on centralized support teams because of complexing and large number of systems. What's needed is a way to simplify remote management of many by a central support team, while ensuring security – and fully automating recurring incident resolution to minimize downtime and interruptions.



Example diagram of a leading fast food chain orchestrating Edge automation with the PagerDuty Operations Cloud across its cloud stack and multiple physical stores and devices.

Reduced interruptions and **increased capacity** across local and remote environments

Revenue is enhanced due to reductions in incidents, missed SLAs, and unplanned downtime.

Improved time-to-value across local and remote environments with automated operations

Improved security by baking access control into automation and connect high-security edge devices across environments

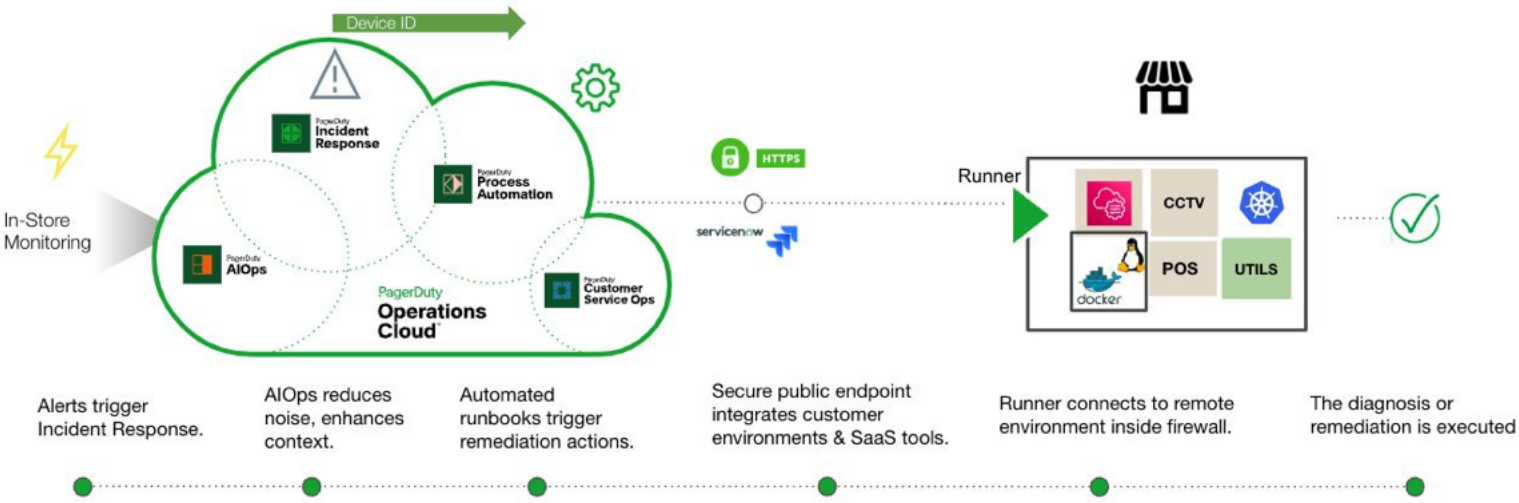
Costs are reduced as a result of automating away the toil of repetitive manual tasks

Enhanced efficiency and availability by eliminating recurring toil across teams

How it works

PagerDuty

With enhanced connectivity to the PagerDuty Operations Cloud, responders can centrally run an incident response and invoke automated operations as needed across secure, hybrid, and edge environments. Combining the use of PagerDuty AIOps, PagerDuty Incident Response, and PagerDuty Process Automation, teams are able to manage, run, and resolve the entirety of an incident from a single, central orchestration plane. Combining the power of the Operations Cloud and the versatility of edge computing, teams have the ability to embed automation into every facet of their operations, enabling cost reduction, better security, and operational efficiencies across the board.



Monitoring tools amd integrations allow Operations Cloud to take in all your monitoring and observability signals to detect incidents

PagerDuty AIOps uses built-in ML models to reduce noise and add granular context for responders to help find true incidents and repress unnecessary alerts.

PagerDuty Process Automation enables creation and execution of automated runbooks that execute diagnostic & remediation actions.

Secure public endpoint for connecting to Runner agents deployed in customer environments, as well as other cloud service such as ServiceNow or Jira Cloud.

Zero trust-compliant runner agent securely connects Operations Cloud to nodes within remote environments to facilitate orchestration steps. Runner sits inside firewalls communicating through HTTPS, allowing otherwise locked-down access.

Orchestrated automation calls local commands, scripts and APIs in order to diagnose or remediate a problem, resolving the incident automatically from remote.

Example jobs:

- Surface specific application and VPC logs.
- Update local firewall for Kubernetes pod changes
- Device restarts and system reconnect
- Retrieve logs from pods by selector label, restart POS system, reconnect CCTV device(s)

For more information, visit pagerduty.com/platform/automation/process-software/