

Online Travel Services Leader Agoda Hyperautomates Cloud Security with Torq

47% Reduction **3 Days**

In missed SLOs

Reduction in time to deliver a solution

Critical Success Factors

When looking to advance its cloud security, Agoda's Application Security team sought to:

Lower the overall organizational cost for maintaining the growing cloud assets while keeping them secure

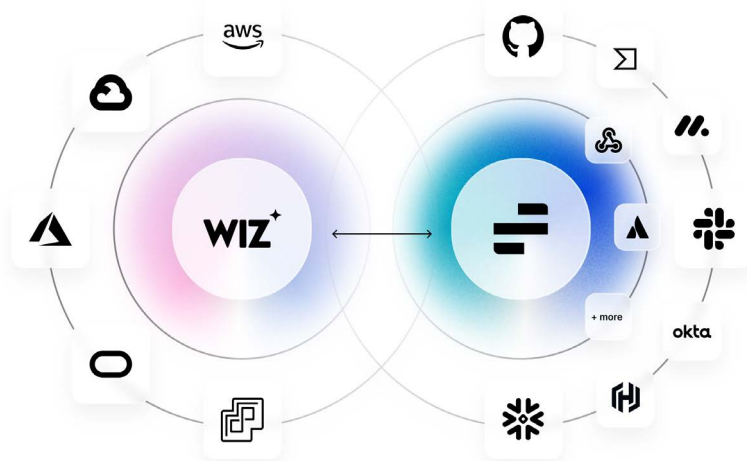
Reduce the MTTR (Mean Time to Resolve) for cloud security findings risks.

Streamline the process related to human interaction / involvement (as resolving cloud security issues requires interaction with multiple software development and DevOps teams spread across multiple countries and timezones)

Operate the solution successfully with a geographically distributed team, limited

Connect the Cloud Security program to the SOC Continuous Vulnerability Management Program, leveraging the existing Vulnerability Management dashboard, resulting in less overhead in managing data conversion resources, skills and time

Hyperautomated System Architecture



About Agoda

BACKGROUND

Agoda helps anyone travel anywhere with its exceptional-value deals on a global network of 2.9M hotels and holiday properties worldwide, plus flights, airport transfers, and more. Agoda.com and the Agoda mobile app are available in 39 languages, and supported by 24/7 customer support.

FOUNDED

2005

HEADQUARTERS

Singapore

REGION

Worldwide

OF EMPLOYEES

5,500

SPECIALTIES

- Vacation rental, hotel, flight, and airport transfer booking
- Affiliate Partners Program and development platform

Optimizing with Torq

Torq Hyperautomation tightly integrated with Agoda's Cloud Security Posture Management solution, Wiz, and additional components in Agoda's security stack. The findings detected by Wiz flow into Torq's hyperautomated workflows that orchestrate the set of activities required to enrich and classify the findings, and drive them to resolution.

The main challenge originated from organizational structure complexity. This involved a team of cloud security specialists (architects), which act as a security owner and consultant to multiple projects, owned, in turn, by geographically-dispersed teams. All of them worked within significant time differences.

Outcomes

With Torq, Agoda's Application Security Architects managed to improve their processes and drive cloud security issues to resolution, while gaining the following important benefits:

Productivity

Streamlining processes that would take two-to-three weeks to converge (from the identification of a Cloud Security Posture issue to complete resolution and verification) to near-real-time. It turned "bi-weekly cadences" into a continuous pipeline that promotes handling of important issues without delay.

Extensibility

Allowing a small security team of architects aligned to multiple projects and to handle large amounts of tasks, focus on critical findings, and reduce alert fatigue.

The following benefits were seen through Torq Hyperautomation:

Reduced time from idea to production, due to Torq's intuitive experience

Building hyperautomation strategies that consolidate people, processes, and technologies into coherent solutions

Raising the confidence in analysis and prioritization of security issues

Improving the SLA for security issues resolution and strengthening of cloud security posture

agoda
●●●●●

"Agoda decreased the time from detection and reporting to the engineering team from 2 weeks to almost real-time."

Jemuel Dalino,
Application and Engineering
Security Manager

With this approach, the Agoda Application Security team has implemented the following processes:

Automated Oversight of Cloud Security Posture Trends With Orchestrated Pipeline

The solution was to introduce a shared notification and orchestration pipeline, outlining the critical issues for handling and orchestrating the remediation lifecycle with the involvement of engineering teams owning the relevant assets.

Automatic "Blast Radius" Analysis and Security Issue Prioritization

The solution was to automate checking of a finding "context" by automating the Wiz Security Graph and additional Attack Surface Management data, and prioritize the severity and criticality of findings in a "close to real-time" fashion without human involvement.

Ready to Hyperautomate?

See how Torq can provide your organization enterprise-level security for modern cyber threats.

[Schedule a Demo](#)

