

Case Study

# Large software company leverages AWS to rapidly scale



# *The* **Highlights**



Leadership are now confident in the company's ability to scale up operations to meet demand.

Cost of delivery per customer decreased.

Application response times were reduced to ~30 milliseconds.

CPU utilisation rates dropped from 25 percent to 12 percent.

Moved from releasing updates once every two weeks to continuous daily releases.

Standardisation and automation using AWS CloudFormation significantly increased velocity by minimising the burden on operations.

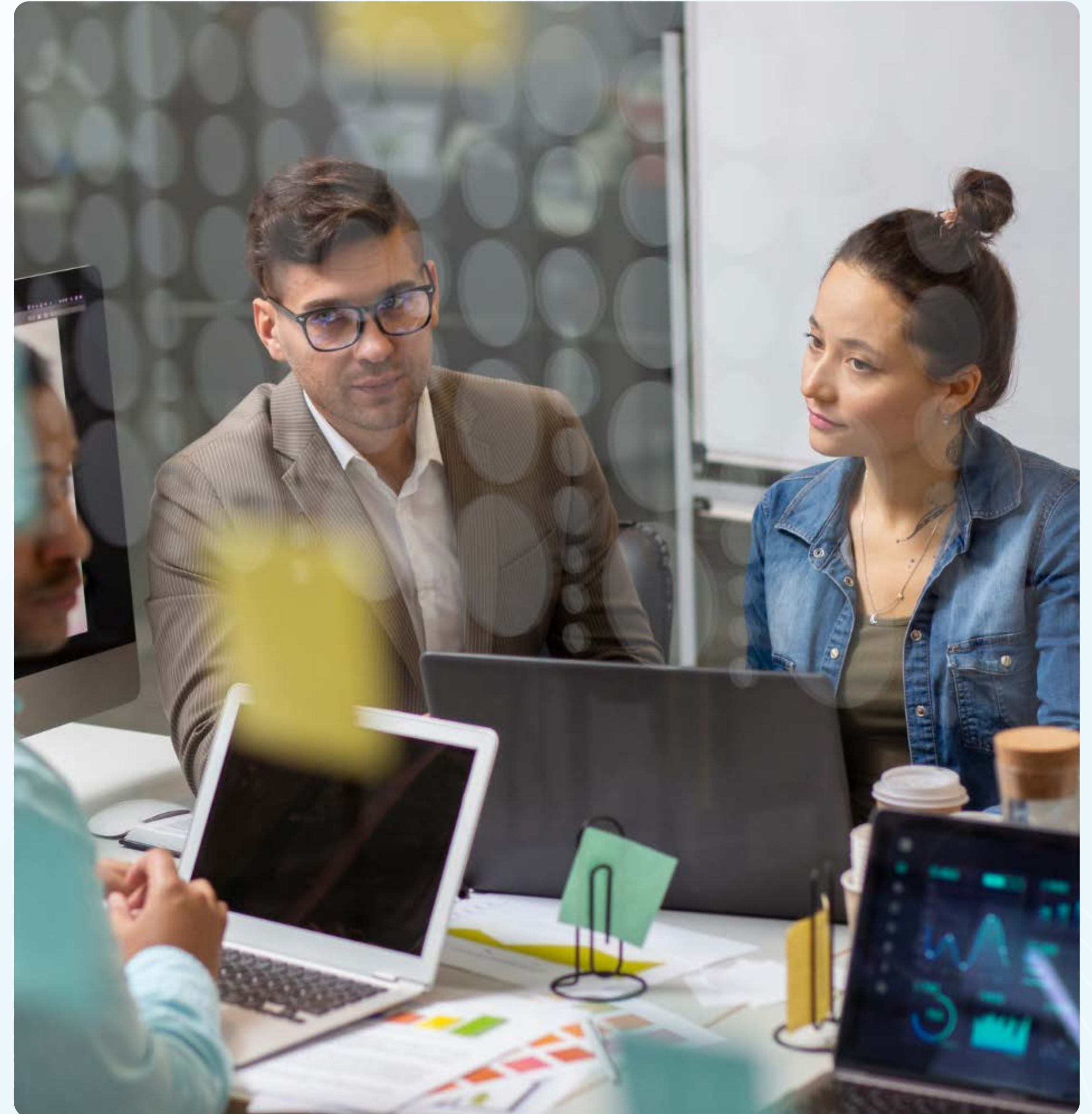
# *The* **Problem**

**Malicious bots represent a rapidly increasing threat to online businesses. On average, 40 percent of login attempts to company websites are fake. This has led to a rise in bot mitigation as a service.**

A large bot mitigation company was experiencing rapid growth and needed to adapt its bot-protection software to be able to handle extreme spikes in traffic – from 10,000 requests per minute to 1 million requests the next.

Though headquartered in Australia, the company has a growing customer base in the US, where businesses tend to incur much higher levels of web traffic. Scaling is critical, as bots swarm these customers' websites when they launch a new product. Left unmitigated, bot attacks can bring a website down for hours, even days.

The company needed to run its operation more efficiently at scale, increase the velocity of deployment, and improve DevOps practices with an automated continuous integration/continuous development (CI/CD) pipeline.





# *The* Opportunity

The rapid growth in demand experienced by this bot mitigation company presented an opportunity to build a robust, scalable infrastructure engineered to keep up with both present and future volume. This would allow the company to expand its customer base in the US and capture industry growth in a cost effective manner, providing a distinct advantage against less scalable competitors.

# The Solution

## The solution implemented by the bot mitigation company was a comprehensive modernisation of their operations on Amazon Web Services (AWS).

The company transitioned from a single-tenant, monolithic architecture to a multi-tenant, microservices architecture. Containerisation was introduced using Elastic Container Service (Amazon ECS) and Amazon Elastic Kubernetes Service (Amazon EKS) for container orchestration.

AWS CloudFormation was implemented to provision infrastructure as code. Security and compliance measures were codified in alignment with the Payment Card Industry Data Security Standard (PCI DSS) and SOC 2 auditing framework. Automation was implemented for the onboarding of new customers (using an AWS Landing Zone with AWS Control Tower).

*The benefits of this solution are as follows:*

### ✓ Improved Scalability

The transition to a microservices architecture and the use of AWS services for container orchestration allowed the bot mitigation company's systems to efficiently handle extreme spikes in web traffic.

### ✓ Reduced Costs

The shift to a microservices architecture, optimisation of resources, and strategic use of AWS services contributed to a significant reduction in the cost to serve each customer.

### ✓ Increased Deployment Velocity

The transformation of their CI/CD pipeline and the implementation of AWS CloudFormation enabled the bot mitigation company to deploy updates more frequently, enhancing their adaptability to bot attacks.

### ✓ Enhanced Security and Compliance

The company enhanced its security posture and ensured compliance with industry standards by codifying security measures and using AWS services for automated threat detection and access control.

### ✓ Faster Response Times

The solution resulted in reduced application response times to about 30 milliseconds – crucial for preventing attacks from sophisticated bots.

# Our Approach

## ... Part 1



### ✓ Engagement of Mantel Group

To begin, the bot mitigation company partnered with Mantel Group to assist in the modernisation of their system infrastructure. Mantel Group provided both strategic and implementation-based expertise, particularly around Kubernetes, to support the company's decision-making process.

### ✓ Transition to Microservices Architecture

With engineering assistance from Mantel Group, the bot mitigation company began transitioning from a monolithic, single-tenant architecture to a microservices, multi-tenant architecture. This shift was designed to reduce the cost per customer and remove interdependencies that could hinder scaling.

### ✓ Optimisation of Resources

The bot mitigation company and Mantel Group conducted extensive work to find the optimum balance between the number and type of instances used, as well as the limit of containers on each instance. This was crucial for efficient resource utilisation and cost-effectiveness.

### ✓ Use of AWS Services for Container Orchestration

The bot mitigation company adopted Amazon Elastic Container Service (Amazon ECS) and Amazon Elastic Kubernetes Service (Amazon EKS) for container orchestration. These services allowed the company's systems to autoscale on demand, adapting to traffic spikes efficiently.

### ✓ Transformation of CI/CD Pipeline

The bot mitigation company transformed its Continuous Integration/Continuous Deployment (CI/CD) pipeline, streamlining its DevOps practices. This allowed for a shorter release cycle, enabling the company to deploy updates more frequently and adapt quickly to bot attacks.

# Our Approach

## ... Part 2



### ✔ Implementation of AWS CloudFormation

The bot mitigation company implemented AWS CloudFormation to provision infrastructure as code. This helped increase deployment velocity by automating and standardising the creation and management of AWS resources, reducing the operational burden.

### ✔ Codification of Security and Compliance

As part of its modernisation, the bot mitigation company codified security and compliance measures in alignment with the Payment Card Industry Data Security Standard (PCI DSS) and SOC 2 auditing framework. This was crucial for maintaining trust with their customers and ensuring they met industry standards.

### ✔ Use of AWS Services for Security

Mantel Group helped implement services such as AWS Security Hub, AWS Config, and Amazon GuardDuty to automate threat detection and access control. This helped enhance the company's security posture and maintain compliance.

### ✔ Standardisation and Automation

The bot mitigation company standardised and automated its operations, including the onboarding of new customers. This was facilitated by the implementation of an AWS Landing Zone with AWS Control Tower, which standardised governance and agile best practices across the company's IT environment.



# Reach out today

We're always keen to start new conversations on using technology to impact people in a positive way.

Contact Us [↗](#)