threatdefence_

CASE STUDY

zip.co

A LEADING INTERNET PAYMENT ORGANISATION BOOSTS THEIR SECDEVOPS CAPABILITIES WITH THREATDEFENCE

Zip Money is an Australian public limited financial technology company. The company was founded in 2013 and is headquartered in Sydney. It currently has around 24,500 retail partners and over 2,100,000 customers in Australia. Zip Money is a highly innovative organisation running cloud native applications and maintaining a very dynamic, constantly changing and evolving environment with hundreds or virtual workloads in multiple public cloud instances.

Hosting sensitive customer data, and processing numerous financial transactions daily, Zip is an attractive target for the most experienced hacker teams worldwide, therefore the ability to detect cyber threat and being able to respond is paramount to Zip. The nature of Zip business leaves no chance to traditional security vendors, as they cannot keep up with the innovation and ongoing changes in the environment.

> *"I cannot endorse this product enough! ThreatDefence provides a top class solution that continuously finds and clearly defines our top risks. Great integration capabilities and tailored functionality makes it a winner."*
>
> **Peter Robinson, Head of Security, Zip Money**

Zip selected ThreatDefence for their tremendous integration capabilities and ability to integrate into Zip's DevOps toolchain end-to-end, satisfying even the most complex requirements and delivering forward-thinking security capabilities. ThreatDefence teams serves as a fully functionable extension of Zip, delivering not only the platform, but also ongoing threat intelligence, detection and incident response.

One of the main challenges for Zip was achieving visibility across their entire cloud infrastructure estate. Hosting numerous workloads around the globe, Zip needed to know exactly how many services are active in the cloud, what was their security configuration, and if it was it adequately protected with their security

defences at any particular moment in time. One of the biggest issue Zip had was inability to automatically discover all cloud instances, taking into account all modern cloud infrastructure features such as auto-scaling workloads.

In addition to continuous, context-rich detection and response across the entire cloud infrastructure of Zip, ThreatDefence also provided Zip with real-time security assurance capability. Enabling ongoing monitoring of security configurations on-premises and in cloud, as well as detection of vulnerabilities and weaknesses in the external perimeter and in Zip's partner organisations, ThreatDefence provided proactive context on external threats, before they could even get a chance to reach Zip's infrastructure.

ThreatDefence integrated into the Zip infrastructure with the use of a scalable API for continuous, automated scanning of all cloud assets, classifying them per business account, and proactively identifying what was exposed to the Internet. ThreatDefence also provided a real-time detection of third party risks, identifying security exposures through thousands of Zip vendors.

Now, Zip is not only able to detect security threats proactively, but also can provide continuous assurance to the business that the environment is secure and protected. At any moment in time, Zip can get a real-time view into their entire infrastructure, review all systems and services from the security perspective, and identify any weaknesses or exposures into their business environment, such as:

- Vulnerable systems
- Shadow IT
- Misconfigured cloud workloads
- Cloud security groups with generous settings
- Security threat indicators
- Anomalous or suspicious behaviour
- Missing security safeguards, as baselined against CIS cloud benchmarks
- Third party risks and exposures.

Equipped with this information, Zip is now able to detect the most pressing security issues in near real time, and quickly uplift security controls to achieve better security posture in a very scalable manner.

threatdefence_

ABOUT THREATDEFENCE_

ThreatDefence provides innovative MDR, SOC-as-a-Service, and proactive cyber defence solutions to MSPs and Enterprises. Our Adaptive XDR Platform was created to help companies of any size to deploy a world-class detection and response, embracing all information that businesses can reach to, would it be within their network, on the Dark Web, or hiding deep into their supply chain. We believe in open ecosystems and connect you to any and all threat intelligence feeds and log sources, instantaneously providing you with actionable security insights. For more information, visit www.threatdefence.com.