

OMNYWAY USES CLOUDGUARD POSTURE MANAGEMENT TO PROVIDE SECURE DEVOPS FOR ITS RETAIL MOBILE PLATFORM



Customer Profile

Omnyway is a born-in-the-cloud advanced mobile shopping and payment platform that provides retailers with the ability to offer their customers a complete digital shopping experience with the use of their smartphone for all aspects of their buying journey.

Challenge

- Visibility into the security infrastructure at scale to better secure their AWS environment.
- Provide flexible access to ports for their developers and yet maintain maximum security
- Automate scanning of its environment that provided continuous compliance reporting along with security best practices.

Solution

- Check Point CloudGuard Posture Management Clarity
- Check Point CloudGuard Posture Management Active Protection
- Check Point CloudGuard Posture Management Compliance and Governance

Results

- Accelerated time-to-market using comprehensive security and compliance automation solutions
- Provided DevOps team with timelimited, on-demand access to services and ports, enabling platform innovation
- Automated continuous compliance for easy identification of issues to quickly correct them

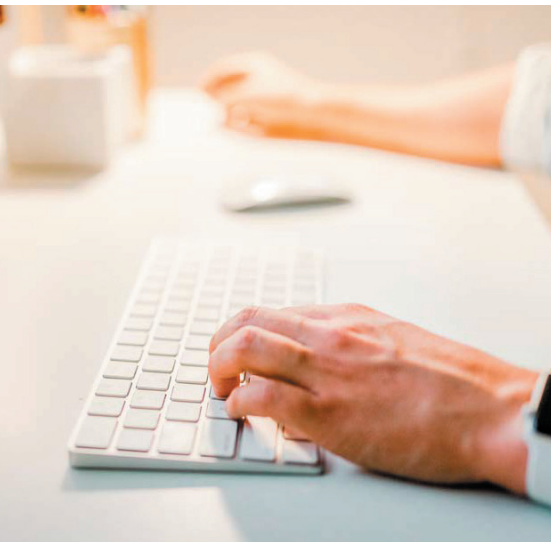
"Speed is a key benefit in secure DevOps, but teams often think that there's a tradeoff between speed and security. That's not always the case. With CloudGuard Posture Management's Dynamic Access Leases, we were able to provide just-in-time access for our DevOps teams to allow for rapid yet secure access which was a major enabler for our IT operations."

-Robert Berger, CTO & SVP Engineering, Omnyway

Overview

Omnyway is a born-in-the-cloud advanced mobile shopping and payment platform that provides retailers with the ability to offer their customers a complete digital shopping experience with the use of their smartphone for all aspects of their buying journey. Omnyway's solution enables their customers to be more competitive by creating a dynamic digital channel between the retailer and shopper across all levels of interaction including in-store, online, in-app, virtual aisle and dynamic media. Omnyway's platform is designed to interface with a retailer's existing system and mobile app with minimal development needed to turn a traditional retail store into a first-class shopping experience for its customers. Omnyway's customers consist of several of the Fortune 500 retailers and is headquartered in Redwood City, CA.

Omnyway's first product was developed for Kohl's department store and provided rewards and special offers as well as payment services. This original product used Amazon Web Services (AWS) EC2 instances



along with relational database services (RDS). The original platform has since evolved, moving away from instances to take advantage of the newer managed services offered by AWS which include microservices architecture, docker containers, the use of Fargate and elastic container service (ECS), Lambda functions, key management service (KMS), and managing IAM policies with simple system manager (SSM) parameters.

Premise

The fact that Omnyway is PCI certified drove us to think about cloud security from the beginning,” said Robert Berger, CTO & SVP Engineering. “We were looking for specific tools to enhance our security and compliance. As our platform channel continued to grow with more applications being developed, our environment was becoming very complex. It was becoming difficult to visualize our VPC peering, security groups and workflows to verify our environment was secure. We also needed a secure yet flexible way to accelerate our DevOps by providing developers with easy remote access while making sure ports remained closed when not in use. Additionally, we wanted to ensure robust security within our platform and wanted a way to consistently scan our environment to provide reports on compliance status along with security best practices, showing us where we could improve. We were looking for a public cloud security solution that would address these concerns, while being future-built to secure existing and new microservices.”

Omnyway’s AWS cloud environment consists of 2 regions, 4 accounts and 20 VPCs that support different applications, with applications being spread across all 4 accounts. The VPCs are designed to isolate specific information that does not need to be shared. All applications are replicated in the second region for resiliency and redundancy so if one region fails, coverage continues. In working with customers and credit card payments, Omnyway’s system is PCI certified but goes beyond the required PCI levels of security. Their frontend system never sees credit card data and the back end uses VPCs to segregate crucial data, with the additional use of AWS CloudHSM security service for an extra level of protection for their data in meeting PCI regulatory compliance requirements.

Business Challenge

Visibility into Security Infrastructure

“As we continued to build our platform and scale in the cloud, our security groups became very complicated and it was hard to track workflow”, said Marius Ducea, VP of Operations. “We needed clear visibility into our security infrastructure to locate misconfigurations and see where items were blocked to fix and secure our environment.”

CloudGuard Posture Management Clarity

One of the key reasons why Omnyway selected CloudGuard Posture Management was for its powerful network security visibility at scale.



"CloudGuard Posture Management provides self-service, fine grained access control to both groups, without isolating the teams. For access to services that are more critical, my security team can control access. The amount of noise we were experiencing with our SIEM has also diminished."

— Robert Berger, CTO & SVP Engineering Omnyway

The CloudGuard Posture Management platform's visualization tool, CloudGuard Posture Management Clarity, provided Omnyway with granular visibility into their network topology and workflows so that they could see their VPC peering and security groups in locating vulnerabilities and remediating them in-place. Additionally, they were able to use the VPC flow log feature in helping identify any misconfigurations, which was crucial in troubleshooting flow issues and debugging in the initial design of their system.

Secure Access for Agile DevOps

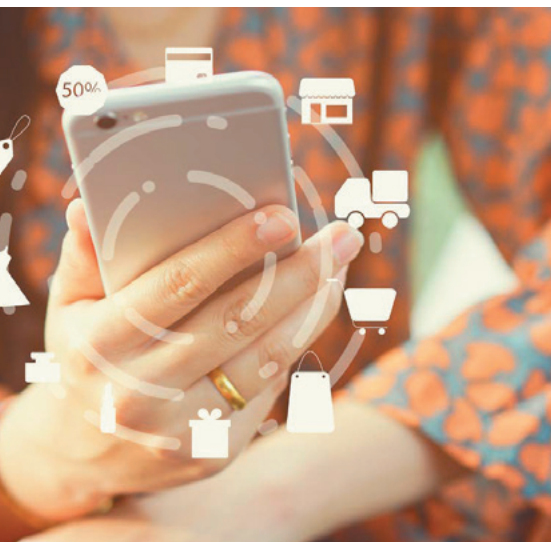
Omnyway was providing developers access to their production environment through their bastion host. With the bastion host open, and a port always exposed, they were consistently experiencing brute force attacks. Additionally, they would encounter a large amount of noise from their SIEM that monitors their logs that would keep generating alerts due to all the attacks. Omnyway wanted to provide flexible access to ports for their developers, making sure the ports were closed after use and a way to minimize alerts to key events.

CloudGuard Posture Management Dynamic Access Leases

CloudGuard Posture Management offers comprehensive network security that goes beyond monitoring and assessment to offer active protection to enforce wanted policies and access control. CloudGuard Posture Management's Dynamic Access Leases was able to provide Omnyway's DevOps team with time-limited, on-demand access to services and ports, that once the lease had expired, would close the port by default. This feature removed the need for using a bastion host and helped reduce the potential attack surface while still allowing legitimate users to get the access they need with the click of a button. According to Robert Berger, CTO & SVP Engineering, "Dynamic Access Leases provides me with a feeling of comfort with only a single person's IP address able to gain access for a specific amount of time. Being a PCI certified platform requires a separation of duties, traditionally with a big wall between Dev and Ops. CloudGuard Posture Management provides self-service, fine-grained access control to both groups, without isolating the teams. For access to services that are more critical, my security team can control access. The amount of noise we were experiencing with our SIEM has also diminished. Our CloudTrail events are now only triggered when someone is logging on. Dynamic Access Leases has been a key component in providing Omnyway with agile DevOps and a huge benefit in advancing our platform.

Enforcement of Continuous Compliance and Security Best Practices

Omnyway is committed to building the most secure mobile platform for its retail customers that it possibly can. With PCI certification, they must meet specific guidelines in securing their environment. Omnyway has gone beyond what is required and was interested in finding a solution that could not only automate scanning of its environment and generating continuous compliance reporting, but also provide security best practices to suggest ways to heighten security policies to ensure a robust security posture.



CloudGuard Posture Management Compliance Engine

The CloudGuard Posture Management Compliance Engine provided Omnyway with a way to bolster security across their AWS environment. Within the Compliance Engine are several compliance and best practices test bundles that once selected, can be automated and set to run checks at desired times across AWS accounts. The test points to assets that have passed or failed and identifies policy issues that need to be addressed to enhance security best practices. These reports are able to point to the status of new assets when added which has been of great value to Omnyway.

Results

Omnyway is currently looking to expand its channel and is in development of its customer facing service. With the continued growth of their business, they may need to expand into a multicloud environment. Continuing to scale in the cloud with a secure, serverless architecture will continue to be their primary objective. Omnyway will continue to use CloudGuard Posture Management's comprehensive security and compliance automation solutions for their future multi-cloud needs.

[For more information, visit: https://www.checkpoint.com/products/](https://www.checkpoint.com/products/)