EAGERS AUTOMOTIVE SECURES CLOUD, DEVOPS-AND CONFIDENCE-WITH CLOUDGUARD

Organization

Eagers Automotive Limited owns and operates car and truck dealerships throughout Australia and New Zealand.

Challenge

- Gain security visibility across two public cloud environments
- Ensure continuous posture alignment with DevOps best practices
- Enable DevSecOps to build security into code pipeline

Solution

- Check Point CloudGuard Network Security
- Check Point CloudGuard Posture Management

Benefits

- Achieved visibility across AWS and Azure environments with centralized management
- Easily monitor and maintain compliance with ISO and other best practices
- Gained shift-left capabilities to automate code security through gates into production

"Check Point CloudGuard delivers a well-rounded, industry-leading approach to cloud and DevOps security. Best of all, we can manage the entire environment from one place instead of having multiple management interfaces for different parts. That's key for us."

- Mark Nix,
National Information Security, Risk & Governance Manager

Overview

Eagers Automotive Limited provides comprehensive sales, service, and parts for almost every major automotive brand in Australia and New Zealand. Its four lines of business include Car Retailing, Truck Retailing, Property and Investments. The company also has robust DevOps capabilities focused on continuously improving operations and the customer experience.

Business Challenge

Gaining Cloud-Level Visibility

Whether you're looking for a car, want to book a service or need financing for a vehicle, Eagers Automotive has you covered. More than 8,000 employees serve customers across 180 sites in Australia and New Zealand. The company is also transforming the automotive experience with a robust DevOps team focused on dealership apps, mobile apps, and one-stop online car sales. The responsibility of securing everything falls to a team of three security professionals.

©2022 Check Point Software Technologies Ltd.
All rights reserved.
June, 2022

"CloudGuard is great. Some products out there focus only on compliance, some on posture, and some only on DevOps. CloudGuard does it all, and it was the key determinant for us."

- Mark Nix,
  National Information Security,
  Risk & Governance Manager

Eagers Automotive began its journey to the cloud by migrating its on-premises Microsoft Exchange environment to Office 365. Soon afterwards, the IT team began migrating servers to AWS, and more recently, Azure. The cloud gives Eagers Automotive greater agility and makes it much easier to keep systems updated with the latest capabilities. Primary infrastructure has typically been implemented in AWS, but in the past year, Eagers Automotive has begun deploying both infrastructure and development capabilities in the Azure cloud.

"We initially relied on native AWS or Azure cloud security tools," said Mark Nix, National Information Security, Risk & Governance Manager for Eagers Automotive. "We could scan for vulnerabilities in each cloud environment, but the native tools didn't really cover all of the functions we needed."

In addition to increasing security controls for their cloud-based assets, the team needed better visibility into each environment. Going forward, more applications and in-house development will be moved into the cloud, and the security team needed an easier way to see—and secure—everything.

"We needed a better solution for gaining visibility and ensuring compliance across both AWS and Azure environments," said Nix. "We also wanted shift-left capabilities, so that we can implement security into new development at the code level. We began looking for a new cloud security vendor."

In addition to achieving better visibility and support for secure development, Eagers Automotive wanted a proven vendor with a strong reputation. Management simplicity was also important. With a rapidly growing estate to secure, automation and unified management were essential. After considering several vendors for cloud security and other, separate vendors for DevOps security solutions, Eagers Automotive chose Check Point CloudGuard Network Security and CloudGuard Posture Management.

SOLUTION

Unified Approach for Security and DevSecOps

Check Point CloudGuard provides unified, cloud-native security across applications, workloads, and cloud networks. CloudGuard Network Security's advanced threat prevention protects cloud assets and workloads from the most sophisticated threats across both AWS and Azure environments. The team gained visualization for all cloud traffic, security alerts, assets and auto-remediation from a single platform. Enriched contextual information from multiple log sources delivers fast, clear understanding of events that occur in either cloud environment.

©2022 Check Point Software Technologies Ltd.
All rights reserved.
June, 2022

"CloudGuard visibility is a huge benefit. We can quickly investigate critical alerts, and I can sit with our cloud architect to see everything and make any decisions right then. We know where we stand at any given moment."

- Mark Nix,
  National Information Security,
  Risk & Governance Manager

CloudGuard Posture Management automates governance across multi-cloud assets and services. Now the team can visualize and assess security posture, detect misconfigurations, model and actively enforce gold-standard policies. Complying with best practices is easy with the ability to modify and automate processes.

With CloudGuard, Eagers Automotive can shift left—bringing CloudGuard security capabilities into the CI/CD pipeline to detect and prevent risk in cloud deployments. DevOps teams can scan Infrastructure as Code (IaC) templates for risk, check software for known vulnerabilities, and scan buckets and containers for security issues.

"Check Point CloudGuard delivers a well-rounded, industry-leading approach to cloud and DevOps security," said Nix. "Best of all, we can manage the entire environment from one place instead of having multiple management interfaces for different parts. That's key for us."

Benefits

See Everything, Guess at Nothing

Before CloudGuard, the team's native cloud and open source tools didn't deliver the level of visibility or remediation features needed to confidently push out new development. Now for example, the team can see if an S3 bucket is not encrypted. They can determine the risk associated with that instance. Then, they can manually remediate the issue or automate a process to ensure that every similar instance is remediated the same way. CloudGuard also enables them to visualize network connections to spot potential problems—and remediate them before a security incident occurs.

"CloudGuard visibility is a huge benefit," said Nix. "We can quickly investigate critical alerts, and I can sit with our cloud architect to see everything and make any decisions right then. We know where we stand at any given moment."

Always Aligned, Soon Automated

CloudGuard Posture Management plays several critical roles for Eagers Automotive. The company had made a significant investment in best-in-class DevOps production, shared, and testing environments. Its security policies also are written in accordance with ISO standards.

"It's important to know that we are maintaining best practices to maximize our DevOps capabilities and that our investment is paying off," said Nix. "CloudGuard Posture Management helps us stay aligned with these best practices and makes compliance easy."

Using CloudGuard Posture Management enables the team to easily assess status and remediate any deviations. For example, early issues with securing lambda functions in AWS were quickly identified and successfully addressed.

CHECK POINT

©2022 Check Point Software Technologies Ltd.
All rights reserved.
June, 2022

"Shift left capabilities are critical going forward. We're monitoring code now with CloudGuard and plan to make code security automatic and part of the normal DevOps pipeline".

- Mark Nix,
  National Information Security,
  Risk & Governance Manager

In addition to ensuring compliance with ISO 27001 standards, the team can run compliance checks against other standards for a broad view. The team began by making manual posture adjustments when needed. As they refine their processes, they plan to automate many of them, such as automatically ensuring that S3 buckets are encrypted. Automation will enable the team to ensure that code promoted into the cloud will be a standard build.

"CloudGuard Posture Management gives us the comfort level and simplicity we wanted," said Nix. "We can highlight when something is not within the right posture—and fix it. CloudGuard is so easy to use."

Shift Left, Move Forward

CloudGuard shift left capabilities are replacing the team's previous open source toolsets—and taking them further. Instead of having to review individual code manually or outsource the function, CloudGuard will automatically search for vulnerabilities as code moves through gates to production. If a vulnerability is detected, the code cannot proceed further until it meets the standard required.

"Shift left capabilities are critical going forward," said Nix. "We're monitoring code now with CloudGuard and plan to make code security automatic and part of the normal DevOps pipeline."

"CloudGuard is great," he continued. "Some products out there focus only on compliance, some on posture, and some only on DevOps. CloudGuard does it all, and it was the key determinant for us."

CHECK POINT

©2022 Check Point Software Technologies Ltd.
All rights reserved.
June, 2022