Case Study

aqua

NCR Attains Security & PCI Compliance For Its Container-Based Applications

NCR

Customer Overview

NCR Corporation (NYSE: NCR) is a leading software- and services-led enterprise provider for organizations in the financial, retail, hospitality, telecom and technology sectors in 180 countries. A Fortune 500 company headquartered in Atlanta with 34,000 employees worldwide, NCR develops the software and hardware for its point-of-sale (POS) solutions, ATMs and digital banking products.

The Challenge: Securing the entire dev-to-prod process

Enterprises across industries are aiming to become more customer-facing and adaptable by implementing agile processes for software development and delivery. As a leading technology provider, NCR is at the forefront of this trend. NCR's software development teams have started using cloud native technologies such as microservices and containers to build and ship applications faster than ever, while migrating to public cloud services to reduce infrastructure costs. These changes created security and compliance challenges that could not be addressed with yesterday's security tools.

Customers trust NCR to secure their highly sensitive financial data, so it was cardinal for the company to implement a solution that both ensures the security of applications and data, as well as satisfies strict compliance requirements.

Achieving both goals required that NCR's Application Security and Site Reliability Engineering practices to gain greater visibility and control over their security posture, without compromising on the velocity and scale of this new approach.

The NCR team recognized that the first step is enhancing the visibility into what developers are trying to deploy to production. Developers can then own the remediation path, identifying issues early in development. By sharing issues earlier in the SDLC and supporting the dev teams, you avoid getting into customer delivery issues due to security findings. So the focus had to be on built-in security in development, combined with detecting and stopping intrusions during runtime.

The NCR team reviewed the leading container-native solutions and chose Aqua Security for its ability to provide the needed functionality, and more importantly, as a partner in its journey to implementing cloud native architectures.

The NCR team realized that in such an emerging technology segment, the specific features that a vendor provides are bound to change, so it was important to find a vendor with whom it can establish a long-term relationship, and see its inputs reflected in product releases within months.

The Solution: Automating security across the application lifecycle

The NCR team deployed Aqua in its container development and production environments across multiple pipelines and dozens of development teams. Aqua has enabled the security team to secure the development-to-production cycle using a policy-driven approach that ensures applications are enterprise-ready without hindering the speed of delivery.

With the Aqua platform, NCR was able to automate the steps required to ensure secure application development and deployment practices:

- Scan container images in the CI/CD pipeline and in registries for known vulnerabilities, embedded secrets, and unsecured configurations
- Prevent images with high severity vulnerabilities, root user privileges. Or hard-coded secrets from running anywhere in the environment
- Ensure that running containers don't drift from their originating images
- Enforce runtime controls that detect and prevent non-whitelisted processes and actions
- Create a granular audit trail for PCI-DSS compliance

Aqua Enforcer containers were deployed on NCR's Kubernetes clusters to enable runtime controls and provide ongoing monitoring and intrusion prevention.

As NCR started to migrate some applications to additional cloud providers, including Google Cloud, the transition was seamless since the Aqua central console provides the exact same controls for Google Kubernetes Engine (GKE) deployments as it does elsewhere, managed centrally across cloud platforms and on-prem infrastructure.

Benefits: PCI compliance and automated full-lifecycle security

Several of NCR's applications handle credit card and payment data, and so are subject to regular audits for compliance with the PCI-DSS security standards. After NCR implemented Aqua, its Qualified Security Auditor (QSA) commented that the Aqua solution was very helpful to demonstrate the controls needed to protect customer data.

The PCI auditors were very impressed with Aqua and the fine level of control and visiblity it provided. They liked the fact that everything was tracked from early stages of development to production.

With its end-to-end security automation, Aqua enables NCR to:

- "Shift left" and embed security and compliance checks early in the development cycle
- Gain visibility into the security posture of applications from development to production
- Control the flow of code into production to prevent introduction of vulnerabilities and other security issues
- Enable smooth multi-cloud deployment and cloud migration
- Provide auditors with detailed data for PCI compliance

About Aqua

Aqua Security helps enterprises secure their cloud native, container-based and serverless applications from development to production. Aqua bridges the gap between DevOps and security, promoting business agility and accelerating digital transformation. Aqua's Cloud Native Security Platform provides full visibility and security automation across the entire application lifecycle, using a modern zero-touch approach to detect and prevent threats while simplifying regulatory compliance. Aqua customers include some of the world's largest organizations across sectors ranging from financial services to Internet giants, with global implementations spanning a broad range of cloud providers and on-premises technologies.

contact@aquasec.com
www.aquasec.com
@AquaSecTeam
AquaSecTeam