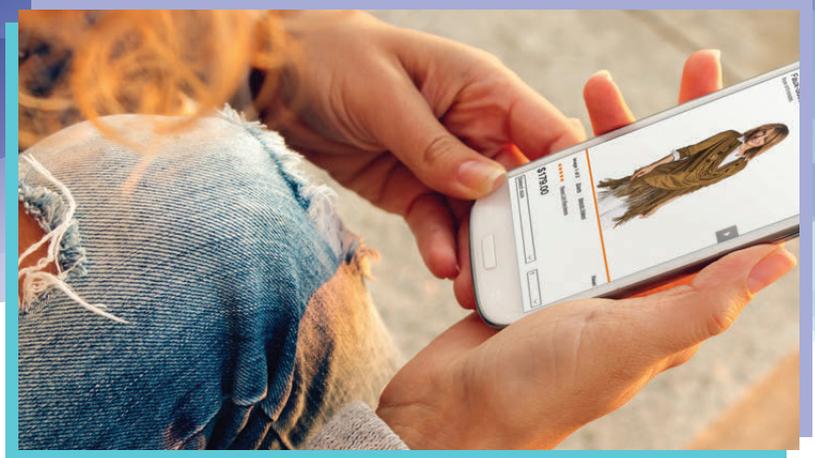# Aptos
Case Study

Aptos provides enterprise software focused exclusively on retail to more than 1,000 brands in 65 countries. Aptos delivers omni-channel commerce and merchandise lifecycle management solutions that help retailers develop dynamic and responsive assortments, streamline operations, and deliver integrated, seamless experiences to shoppers independent of the point of sale (POS).

Aptos is revolutionizing the retail digital transformation with the first offering on its innovative Aptos ONE SaaS platform, Aptos ONE Store Commerce. Leveraging containers and microservices, Aptos has enabled next-generation in-store capabilities for its retail customers, including mobile device support, offline transaction processing, and customer-specific extensions that the retailers themselves can design.

Securing retail customer data

Retail software is an obvious target for hacking. According to a recent study, retailers experienced more breaches than any other industry in 2019, losing more than $30 billion to cybersecurity attacks.[1]

Aptos is using Kubernetes and Docker to support its multi-cloud strategy. To enhance security for these workloads, Aptos is leveraging the StackRox Kubernetes Security Platform.

The StackRox Kubernetes Security Platform enables customers like Aptos to visualize their Kubernetes environments, provides risk profiling across infrastructure, reduces the attack surface, and finds and stops malicious activity.

Aptos is a recognized market leader in retail technology solutions, delivering innovative, cloud-native, and comprehensive omni-channel solutions.

Headquarters:
Atlanta, GA

Founded: 1972

Environment:
AWS, Azure,
Docker, Kubernetes

www.aptos.com

1. https://intsights.com/resources/cyber-attack-monday-hackers-target-the-retail-industry-as-e-commerce-thrives

aptôs

The StackRox platform integrates into the infrastructure DevOps teams depend on – including CI/CD tools, managed Kubernetes services from cloud providers, and registries – and it ties into DevOps workflows to make container and Kubernetes security scalable, practical, and operational.

"The primary value we're getting out of StackRox is proactively discovering and managing vulnerabilities and misconfigurations throughout the infrastructure," says Jason Harris, vice president of cloud architecture and suite management at Aptos. "We're able to evaluate Kubernetes and the containers themselves to identify and remediate those problems, enabling us to continuously harden our cloud-native infrastructure."

Harris continues, "Another StackRox feature that has been extremely helpful is the tie between the configuration management capabilities and compliance. We're able to demonstrate and constantly improve our adherence to industry standards."

StackRox features in practice at Aptos

- **Vulnerability management** – StackRox identifies vulnerabilities in Aptos' images, running deployments, and Kubernetes itself.

- **Configuration management** – Aptos leverages StackRox to identify misconfigurations across images, containers, clusters, Kubernetes, and network policies, preventing accidental exposures that could put the company's systems at risk.

- **Compliance** – Aptos is able to immediately identify any instance that fails to meet its internal policies or industry standards, such as with SOC 2 and PCI.

- **Visibility and control** – StackRox provides comprehensive visibility into Aptos' cloud-native infrastructure, including all images, container registries, Kubernetes deployment configurations, and container runtime behavior.

StackRox

LET'S GET STARTED

Request a demo today!
info@stackrox.com
+1 (650) 489-6769
www.stackrox.com