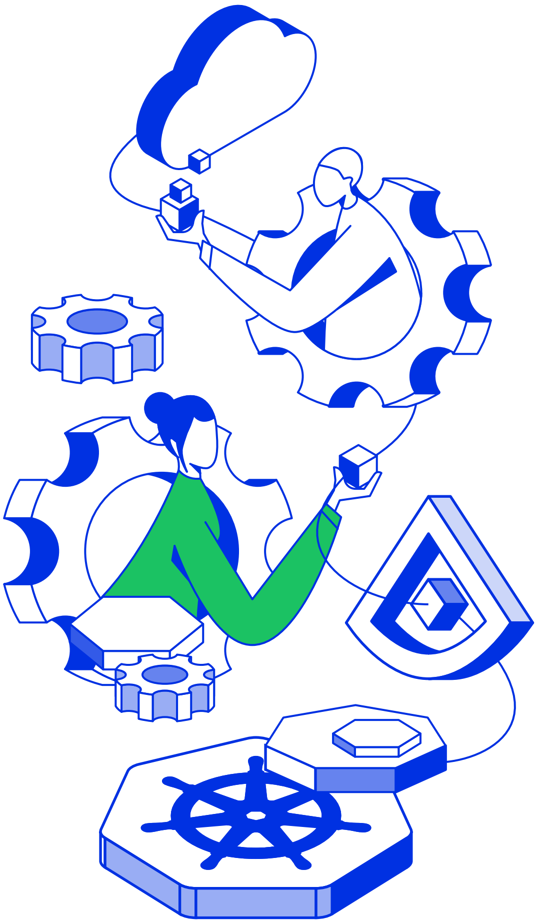
alcide

CASE STUDY DFDS

DFDS USES ALCIDE KUBERNETES ADVISOR & MICROSERVICES FIREWALL TO SECURE CLUSTER DEPLOYMENTS IN A MULTIPLE DEV TEAM ENVIRONMENT

DFDS, a European leader in passenger sea transport, freight shipping and cargo logistics, believes that applying cutting edge technologies to business operations is the driving force behind their success and is crucial for delivering a quality customer experience. To achieve this goal, DFDS built a distributed software architecture with containers and Kubernetes that allowed for autonomous dev teams IT across Denmark, England and Turkey and could be easily scaled to accelerate time to market. From automation, to modularization and connectivity, DFDS's Smart Data department relies on this architecture for all aspects of business operations and customer interactions.



CHALLENGE

DFDS utilises Kubernetes deployment in Amazon Elastic Kubernetes Service (Amazon EKS). They use elastic load balancers for their pubic facing components, and AWS IAM configuration for building their clusters' authentication.

With close to 500 microservices deployments by multiple independent development teams, DFDS understood that visibility, collaboration, as well as fast execution were top priorities for maintaining a successful and secure dev environment. DFDS needed a security solution that could be implemented and tracked across all teams while eliminating the need for an expert on every site.

SOLUTION

After considering a number of available technologies for securing their production pipeline, DFDS decided to implement Alcide's scanning tool, Kubernetes Advisor, as well as Microservices Firewall.

Kubernetes Advisor, a multi cluster vulnerability scanner, combines platform and orchestration policies into one dashboard which equipped DFDS with the ability to easily monitor and manage cloud operations. It covers kubernetes and Istio security best practices, compliance checks, hunting misplaced secrets or excessive secret access, workload hardening, Istio security configuration, as well as API server access privileges. It secures Kubernetes cluster hygiene in CD pipeline, allows for visibility in kubernetes black box in order to detect threats in clusters. Kubernetes Advisor enabled DFDS to get an overview of their many deployments in a secure and automated manner. And repeat that.

Microservices firewall for its part offered DFDS a simplified platform where developers can define network policies during build time, ensuring that the Kubernetes workload will operate normally in runtime. The platform can define network policies according to a number of factors, including IP ranges and external domains while having the ability to manage and visualize all their external policies. The platform consolidates all of their security policies, platform policies and container orchestration policies into one dashboard so that the developers can easily understand inbound and outbound rules as well as enforce policies across their cloud infrastructure and microservices interactions.

RESULTS

Alcide Kubernetes Advisor provided DFDS with continuous live analysis of their kubernetes deployments which included continuous updates of the clusters' risks and hygiene through a detailed list of misconfigurations. They could detect hygiene drifts and reduce noise by spot- on hygiene delta, as well as prevent real-time misconfigurations and block tainted CI/CD pipelines.

Using Alcide Kubernetes Advisor with EKS allowed DFDS to increase its productivity by releasing a secured pipeline without having to postpone their production deployment.

In short, DFDS experienced an increase in productivity through Kubernetes Advisor by securly deploying and monitoring Kubernetes clusters, nodes and pods, and get actionable recommendations to mitigate security risks before they were exploited.

By using Alcide Microservices firewall, DFDS were able to enforce application-aware and label based policies by collecting communication patterns into their centrally orchestrated cloud security policies. It enabled the company to combine all of their policies into one single firewall, unified different clusters into one incident stream, and embed the policy into the workload.

This combination allowed them to optimize for policies management, detection and intelligence, all in one solution.