Tigera Case Study: Mulligan Funding

Calico Cloud enables Mulligan Funding to launch SOC 2 - compliant fintech SaaS platform

MulliganFunding

About

- Business loan provider
- San Diego, CA
- 100-200 employees
- Serves small to medium-sized businesses in the US

Goals

- Scalable security policy management
- Reduced lateral attack surface
- SOC 2 compliance for its cloud SaaS platform

Solution

- Used Calico's Policy Board to manage and deploy all network policies
- Utilized Calico's Dynamic Service and Threat Graph to gain observability and insight
- Used Calico to produce SOC 2 audit and benchmark reports

Results

- Unified security policy management
- Reduced service disruptions
- Strengthened security posture

Background

Mulligan Funding needed to launch a new microservices-based, cloud SaaS platform to streamline its loan-offering services and allow online loan check-outs. Because their SaaS platform would handle sensitive personal and financial data, all communications from and to the application needed to be secure and SOC 2 compliant. To achieve this, Mulligan Funding decided to standardize on Microsoft Azure Kubernetes Service (AKS) and Calico Cloud for security and compliance.

Mulligan Funding needed to re-architect its tech stack to a SOC 2-compliant, Kubernetes microservices-based architecture hosted on Microsoft AKS.

Challenges

Challenge #1: Lack of visibility and scalability

The lack of flexibility and scalability of native Kubernetes policies, which are IP dependent, was a major obstacle to Mulligan Funding's goal of becoming SOC 2 compliant. Since these policies are IP-dependent, Mulligan Funding's microservices communication often broke due to frequent and inevitable IP changes.

Lacking observability into Kubernetes clusters, Mulligan Funding's team had a long troubleshooting process that involved investigating rulesets, access gateways, and comparing IPs and security policies. The troubleshooting process was a "time sink," according to Jeff Puccinelli, Director of Infrastructure and Security Operations at Mulligan Funding. He knew the DevOps team would soon be overrun by frequent security policy errors and violations.

Challenge #2: Preventing unauthorized access at scale

Security threat gaps widened as the company added more partners and needed to provide connectivity to partner environments. At the time, Mulligan Funding had to manually deny policies and whitelist domain names, which is not ideal, given the large attack area within a Kubernetes cluster. Since an attacker can quickly move laterally within a cluster to find sensitive data and high-value assets, Mulligan Funding needed to bolster its security profile at scale.

Copyright © 2022 Tigera, Inc. All rights reserved

It's extremely helpful to know what endpoints your services are talking to. With Calico Cloud in place, we have a much-improved security posture.

JEFF PUCCINELLI
Director of Infrastructure and Security Operations, Mulligan Funding

Solution

Calico Cloud's Dynamic Service and Threat Graph and Flow Visualizer allowed Mulligan Funding to instantly pinpoint specific issues in pods, microservices, and namespace communication. Puccinelli and his team were able to define which microservice or workload can communicate with which external service, all while no longer being IP-dependent.

Mulligan Funding streamlined security policy management and troubleshooting using Calico's Policy Board, which allowed them to stage, preview, and deploy policies without needing to manage them all individually.

Calico Cloud also provided SOC 2 audit and benchmark reports, helping Mulligan Funding achieve the needed compliance status to operate its SaaS platform.

"I can go through and use the Dynamic Service and Threat Graph to drill down to the exact pod to see what it's attempting to talk to, see what policies are applied to it, and figure out why that communication is not happening."

*—**Jeff Puccinelli**, Director of Infrastructure and Security Operations*

Results

After implementing Calico Cloud, Mulligan Funding was able to strengthen its security posture and saw reductions in its service disruptions. Security gaps and violations were found instantly using Calico's Dynamic Service and Threat Graph and Flow Visualizer, and could be troubleshot on the spot. Calico's Policy Board allowed Puccinelli's team to manage, evaluate, and monitor all policies with all necessary correlation and insight in one place. All of this resulted in business partners, banks, and regulatory agencies feeling assured that Mulligan Funding has a proactive, controlled, and zero-trust approach in place for its security.

No longer cluttered by policy management or slowed by security and compliance concerns for its SaaS application, Mulligan Funding is able to focus and further expand its development team to uncover more business opportunities. Puccinelli was also pleased with Tigera's support team: "Tigera's support team has been excellent—their on-call engineers worked with me after hours and solved issues on the spot."

About Calico Cloud

Calico Cloud is the industry's only active Cloud-Native Application Protection Platform (CNAPP) with full-stack observability for containers, Kubernetes, and cloud.

For more information, visit:
https://www.tigera.io/tigera-products/calico-cloud/

TIGERA

Tigera, Inc.

58 Maiden Lane, Fl 5
San Francisco, CA 94108
+1 (415) 612-9546 / www.tigera.io

Copyright © 2022 Tigera, Inc. All rights reserved