TRUEFORT®

SOLUTION BRIEF

Cloud Workload Protection for Kubernetes

Kubernetes orchestrates clusters of virtual machines and schedules containers to run on those virtual machines - based on their available compute resources and the resource requirements of each container.

Kubernetes automatically manages service discovery, incorporates load balancing, tracks resource allocation, and scales based on CPU utilization, thus simplifying many aspects of running a service-oriented application infrastructure.

Kubernetes Security and Observability Challenges

However, Kubernetes has one glaring exposure: By default, it lacks security controls. Containers are grouped into pods, the basic operational unit for Kubernetes, and any pod can talk to any other pod. While some commercial solutions exist that address this shortcoming, they are limited to addressing Kubernetes and cannot be applied to the remaining 90% of IT infrastructure that is outside of the Kubernetes domain.

While Kubernetes is growing rapidly, the amount of Kubernetes infrastructure and applications is dwarfed by existing “legacy” infrastructure. To protect Kubernetes environments, SOC teams have been forced to deploy yet another management platform, introducing more operational complexity and overhead, into already overburdened IT teams.

With the expansion of Kubernetes beyond sandboxes and engineering projects to business-critical commercial deployments by financial services, e-commerce, and other industries, granular application-layer security and visibility have become table stakes. Most open-source and commercial Kubernetes security solutions are focused on the network layer, with limited or no visibility into business-critical application layer behavior.

Default Kubernetes is like a house without locks - open to everyone. Containers may be grouped into pods, but any pod can communicate freely with any other pod or, even more concerningly, with vulnerable OT and legacy IT environments.

SOLUTION BRIEF

TrueFort for Kubernetes: Behavior analytics and microsegmentation

TrueFort has created a microsegmentation solution for Kubernetes container environments that leverages the proven TrueFort Platform consolidated with comprehensive, granular protection for virtual machines and bare metal servers. By telemetry from Kubernetes daemonsets, TrueFort automatically discovers every application and maps all application relationships.

What makes TrueFort's approach to Kubernetes security unique is the ability to correlate process, identity, and network activity with a trusted behavioral profile for every application running on containers. Once the profile has been created, TrueFort is able to detect any deviations from that profile in real-time and enforce microsegmentation policies to block unwanted lateral movement. Now applications and security teams have a single, unified view of application behavior and threat incidents across all environments.

TRUEFORT FOR KUBERNETES - BENEFITS AND FEATURES

- Operators view all events within a Kubernetes context (pod, namespace, etc.) in a dynamic GUI displaying applications and app relationships
- Easily integrates with leading open-source Kubernetes across EKS, AKS, and others
- Works in all application environments within the enterprise: containers, virtual machines, bare metal servers -- on-premises and cloud
- Enables SOC teams to instantly differentiate between normal and anomalous application behavior, and block "out-of-profile" behavior
- Provides a timeline of application behavior and process chains to show when similar anomalies may have occurred for forensic analysis
- Highly performant and scalable: All via single interface

As Kubernetes continues to expand into commercial deployments, the demand for granular east-west traffic visibility and control will grow.

ABOUT TRUEFORT

TrueFort puts you in control of lateral movement across the data center and cloud. The TrueFort Cloud extends protection beyond network activity by shutting down the abuse of service accounts. Founded by former IT executives from Bank of America and Goldman Sachs, leading global enterprises trust TrueFort to deliver unmatched application environment discovery and microsegmentation for accounts and activity.

For more information, visit truefort.com and follow us on Twitter and LinkedIn.

TRUEFORT

3 West 18th Street
Weehawken, NJ, 07086
United States of America

+1 201 766 2023
sales@truefort.com