AKAMAI 솔루션 설명서

Akamai Guardicore Segmentation으로 Kubernetes 시각화 및 보호

Kubernetes(K8s)는 클라우드 데이터 센터에서 애플리케이션을 배포하고 관리하는 데 가장 널리 사용되는 기술 중 하나로, 이전에는 불가능했던 속도와 유연성을 제공합니다. Gartner는 2026년까지 글로벌 기업의 90%(2021년 기준, 40%)가 프로덕션에서 컨테이너화된 애플리케이션을 실행할 것으로 전망합니다. 또한 2026년까지 기업 애플리케이션의 20%(2020년에 10% 미만)가 컨테이너에서 실행될 것입니다.[1] 컨테이너의 인기가 높아지면서 사용자뿐만 아니라 공격자도 컨테이너로 몰려들면서 보안팀은 초기에 미리 준비하지 못했던 도전과제에 직면하게 되었습니다.

새로운 기술, 새로운 보안 과제

K8s 클러스터는 DNS 서비스, 부하 분산, 네트워킹, 자동 확장 그리고 애플리케이션 실행에 필요한 기타 기능 등 완벽한 생태계를 제공합니다. K8s는 기업들이 빠른 혁신과 비용 절감을 달성할 수 있도록 하기 때문에 K8s의 도입률이 높은 것은 놀랍지 않습니다. 하지만 K8s의 장점은 보안을 더 어렵게 만들기도 합니다.

K8s는 본질적으로 플랫 네트워크인데, 각 팟(pod)이 클러스터 내의 다른 팟과 통신할 수 있다는 것을 의미합니다. 공격자는 최초로 침해하자마자 측면으로 이동해 연결된 모든 데이터 센터에 접속할 수 있습니다. 이것은 전형적인 랜섬웨어 공격 프로세스지만, 다른 공격 기법도 같은 전략을 쉽게 활용할 수 있습니다.

2022 Red Hat State of Kubernetes Security Report에 따르면 DevOps, 엔지니어링 및 보안 전문가 300여 명을 대상으로 설문조사를 실시한 결과, 응답자의 93%는 지난 12개월 동안 K8s 환경에서 최소 한 번의 보안 인시던트를 겪었으며, 이로 인해 매출 또는 고객 유출을 경험했습니다.

솔루션: 마이크로세그먼테이션

K8s에서는 애플리케이션 배포라는 개념 자체가 다르기 때문에 다른 보안 방식이 필요합니다. 보안팀이 기존의 보안 솔루션을 단순히 리프트 앤 시프트(Lift & Shift)하기만 하면 이런 새로운 기술에서도 효과적일 것이라 기대할 수 없습니다. K8s 클러스터를 보호하려면 K8s에 맞춰 적합한 방식으로 이루어져야 합니다.

그래서 Akamai는 K8s 클러스터 보안을 집중적으로 지원하기 위해 소프트웨어 기반의 세그먼테이션 솔루션을 제공합니다. 이 솔루션은 레거시 시스템, 클라우드, 온프레미스 워크로드, 컨테이너 등 환경 내의 다른 워크로드에 대해서도 비슷하게 작동합니다. 따라서 기업 전체의 자산을 한 곳에서 시각화하고, 보호하고, 관리할 수 있습니다.

장점

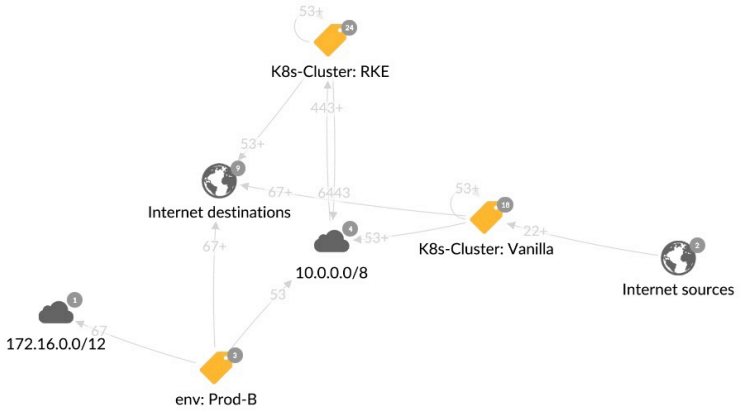
- 다른 자산과 동일한 창 및 프로세스를 통해 K8s 클러스터를 시각화, 적용, 모니터링
- K8s 취약점을 악용하는 정교한 공격을 간단히 방어
- 팟, 서비스, 호스트 또는 네임스페이스 간 모든 연결에 대한 과거 기록 및 실시간 확인 가능
- K8s 클러스터를 쉽게 링펜싱하는 우수한 템플릿
- K8s, 엔드포인트, 온프레미스, 클라우드 워크로드 전반에 걸친 통합 콘솔 및 정책 관리
- 배포된 클러스터에 대한 운영 데이터(모니터링하는 에이전트 수와 Kubernetes 오케스트레이션 상태 등) 수신

Akamai

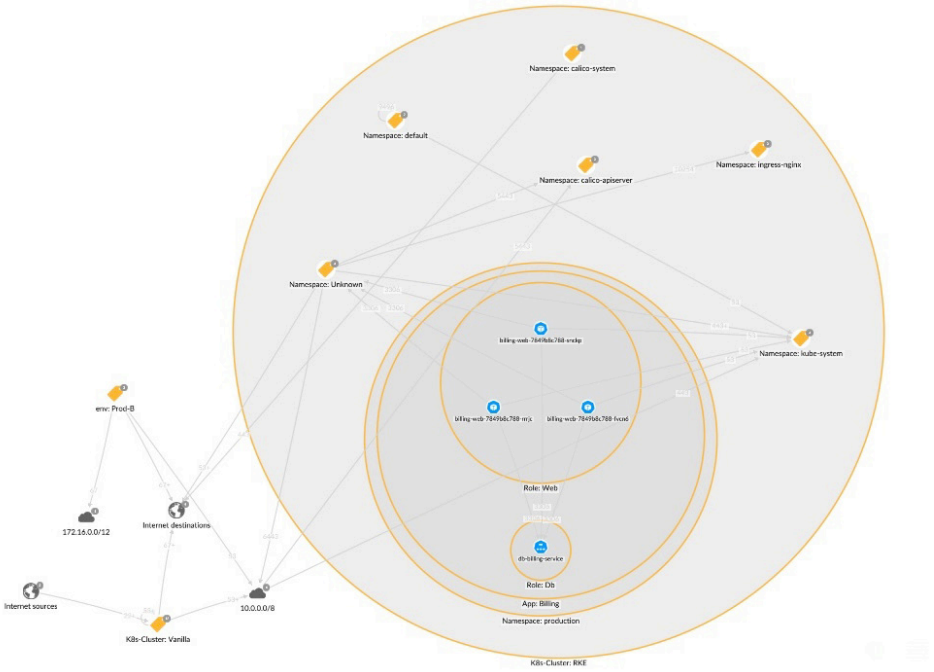
Kubernetes 클러스터를 세그먼테이션하는 핵심 기능

가시성. Akamai Guardicore Segmentation은 K8s 환경에서 무엇이 실행 중인지 파악하고 트래픽이 원하는 방향으로 움직이고 있는지 확인할 수 있는 기능을 제공하는데, 이는 성공적인 정책을 생성하는 데 매우 중요합니다.

- **상호 의존성 맵** - Akamai는 VM, K8s, Docker 컨테이너 등 모든 기술에 대해 내부 통신과 데이터 센터 간 통신을 시각화하는 맵을 제공합니다. 이러한 맵을 통해 팟, 서비스, 호스트 또는 네임스페이스 간의 의심스러운 연결을 시각화하고 탐지할 수 있습니다.
- **레이블** - 맵은 여러 레이블 레이어를 사용해 클러스터에서 애플리케이션이 배포되는 방식을 정확하게 반영합니다. 이 시각화는 앱 관리자가 계획한 대로 K8s 계층을 설명합니다. Akamai 사용자는 이런 세부 정보를 통해 클러스터에 무엇이 배포되었는지 정확하게 파악하고 배포된 앱과 나머지 인프라 사이의 네트워킹 관계를 명확하게 이해할 수 있습니다.



Reveal 맵에 표시된 클러스터. 클러스터를 두 번 클릭하면 네임스페이스 그리고 클러스터 내 네임스페이스의 상호 연결이 표시됩니다.



팟 정보를 표시하는 Reveal 맵

> 응답자의 93%는 지난 12개월 동안 K8s 환경에서 최소 한 번의 보안 인시던트를 겪었으며, 이로 인해 매출 또는 고객 유출을 경험했습니다.

적용. K8s 클러스터에서 공격 표면을 최소화하려면 엄격한 세그먼테이션 정책이 필요합니다. 세그먼테이션 적용 솔루션은 두 가지 주요 기준을 충족해야 합니다. 첫째, 비침입적이고 확장 및 성능 제한이 없어야 합니다. 둘째, 네임스페이스, 컨트롤러, K8s 레이블 등 모든 수준의 K8s 오브젝트를 링펜싱할 수 있는 유연한 방법을 제공해야 합니다.

Akamai는 고유한 Kubernetes CNI(Container Network Interface)를 활용합니다. CNI는 원래 K8s에서 네트워크 세그먼테이션 적용을 위해 설계된 네트워크 보안 정책 플러그인으로 구성됩니다. 확장 제한이 없는 비침입적인 방법입니다. 사용자는 전용 템플릿을 통해 네임스페이스, 애플리케이션, 기타 오브젝트 등 Kubernetes 비즈니스 크리티컬 애플리케이션을 링펜싱할 수 있습니다.

Ring Fence a K8s Application by whitelisting inbound and outbound flows for an application on K8s cluster K8s-Cluster within Namespace

Kubernetes 애플리케이션 링펜싱 템플릿

고급 모니터링. 고급 로깅 및 모니터링 시스템을 사용해 전용 네트워크 로그가 K8s 네트워킹에 맞게 조정됩니다. 모든 이벤트에 대해 대상 서비스, 노드 IP, 소스 및 대상 포트, 프로세스가 표시됩니다. 이를 통해 네트워크에서의 비정상적 활동을 간편하게 조사하고 SIEM과 같은 써드파티 애플리케이션으로 데이터를 내보낼 수 있습니다.

요약

Kubernetes는 많은 비즈니스 환경에서 필수적인 부분이 되었습니다. 기존과는 다른 접근 방식을 사용해 리소스의 효율적 사용, 개발 프로세스 간소화, 이동성 및 확장성 향상을 지원합니다. 애플리케이션 개발 방식이 달라졌다면 보안도 다른 방식으로 접근해야 합니다.

Akamai Guardicore Segmentation은 하나의 맵에서 베어 메탈, VM, K8s 등 다양한 배포 유형에 따른 통신 흐름 전반을 확인할 수 있는 하나의 종합 솔루션을 제공합니다. 비침입적이고 확장 가능한 K8s 고유의 접근 방식을 통해 시각화, 모니터링, 적용을 진행하기 때문에 보안 및 개발팀의 부담을 경감시킬 수 있으며 기업이 보안을 희생하지 않고 신속하게 혁신할 수 있습니다.

2022 Red Hat State of Kubernetes Security Report에 따르면, K8s를 사용하는 가장 큰 이유 중 하나가 보안이며, 보안 문제는 애플리케이션을 프로덕션에서 배포하는 것을 지속적으로 지연시킵니다.

자세한 내용은 akamai.com을 방문하거나 **Akamai** 영업 담당자에게 문의하시기 바랍니다.

1. Gartner, The Innovation Leader's Guide to Navigating the Cloud-Native Container Ecosystem, Arun Chandrasekaran, Wataru Katsurashima, 2021년 8월 18일.

 | 지원 | 2022년 9월 발행