RESUMO DA SOLUÇÃO DA AKAMAI

Visualize e proteja o Kubernetes com a Akamai Guardicore Segmentation

O Kubernetes (K8s) continua sendo uma das tecnologias mais amplamente adotadas para implantar e gerenciar aplicações em data centers nativos da nuvem, oferecendo um tipo de velocidade e flexibilidade que nunca eram possíveis antes. De acordo com o Gartner, até 2026, 90% das organizações globais terão aplicações conteinerizadas em produção, em comparação a 40% em 2021. Além disso, até 2026, 20% de todas as aplicações empresariais serão executadas em contêineres, em comparação a menos de 10% em 2020.[1] A crescente popularidade dessa plataforma tem atraído não só os usuários, mas também os invasores, forçando as equipes de segurança a enfrentar desafios para os quais não estavam inicialmente preparadas.

Nova tecnologia, novos desafios de segurança

Um cluster do K8s fornece um ecossistema completo, incluindo serviços de DNS (Sistema de Nomes de Domínio), balanceamento de carga, rede, escalonamento automático e qualquer outro recurso necessário para executar aplicações. Não surpreende que o K8s esteja sendo adotado tão amplamente, pois ele permite que as empresas obtenham inovação rápida e economia de custos. No entanto, os mesmos atributos que tornam o K8s tão atraente também fazem com que seja mais desafiador protegê-lo.

Trata-se de uma rede inerentemente simples, o que significa que cada pod pode se comunicar com qualquer outro pod dentro do cluster. Após uma violação inicial, os invasores podem se mover lateralmente e obter acesso a todos os data centers conectados. Esse é um típico processo de ataque de ransomware, mas a mesma estratégia pode ser facilmente aproveitada por outro vetor de ataque.

De acordo com o Relatório de segurança State of Kubernetes da Red Hat de 2022, que entrevistou mais de 300 profissionais de DevOps, engenharia e segurança, 93% dos entrevistados sofreram pelo menos um incidente de segurança em seus ambientes do K8s nos últimos 12 meses, às vezes levando a perda de clientes ou receita.

A solução: microssegmentação

Em si, o conceito do K8s de implantação de aplicações é diferente e requer métodos de segurança diferentes. As equipes de segurança não podem simplesmente copiar uma solução de segurança existente e esperar que ela funcione com essa nova tecnologia. A proteção de clusters do K8s deve ser feita de modo nativo ao K8s.

É por isso que a Akamai oferece uma solução de segmentação baseada em software que tem suporte dedicado para proteger clusters do K8s. A solução atua de maneira semelhante para outras cargas de trabalho em seu ambiente, incluindo sistemas legados, nuvens, cargas de trabalho locais e contêineres. Como resultado, você pode visualizar, proteger e gerenciar ativos em toda a sua empresa por meio de um único painel.

Benefícios

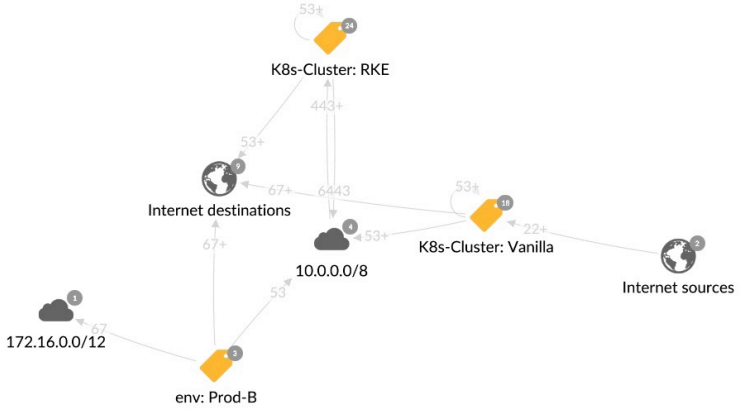
- Visualize, aplique e monitore seus clusters do K8s através do mesmo painel e dos mesmos processos que qualquer outro ativo
- Proteja-se facilmente contra ataques avançados que exploram vulnerabilidades do K8s
- Obtenha uma visualização histórica e em tempo real de todas as conexões entre pods, serviços e hosts ou namespaces
- Obtenha modelos prontos para uso para proteger facilmente clusters do K8s
- Obtenha um gerenciamento unificado de consoles e políticas em cargas de trabalho do K8s, de pontos de extremidade, locais e na nuvem
- Receba dados operacionais sobre os clusters implantados, incluindo o número de agentes que os monitoram e o estado da orquestração do Kubernetes

Akamai

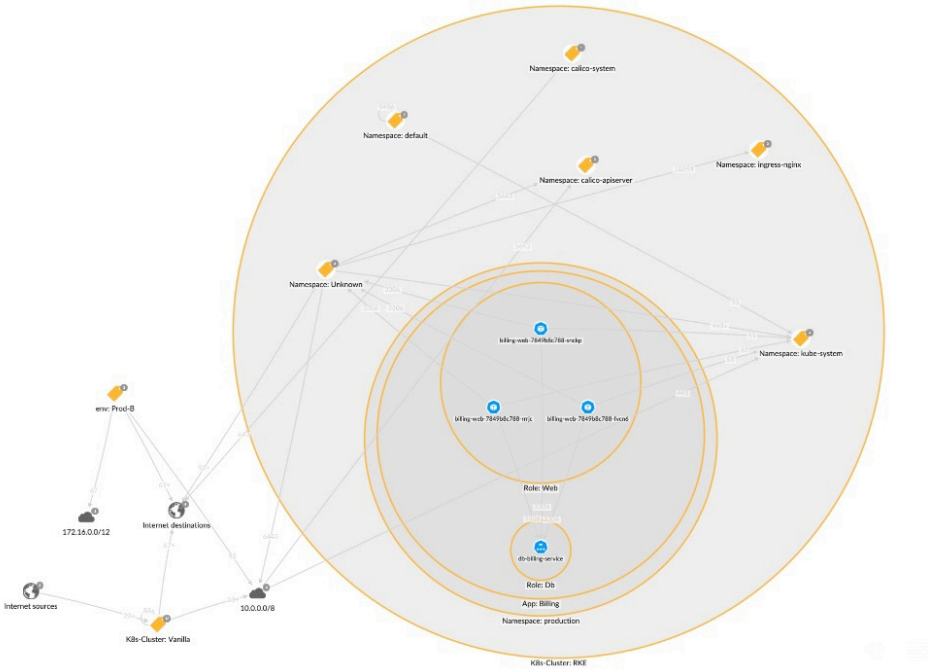
Principais recursos de segmentação de clusters do Kubernetes

Visibilidade. A Akamai Guardicore Segmentation oferece a capacidade de saber o que está sendo executado em seu ambiente do K8s e de confirmar que seu tráfego está indo somente para onde você deseja, o que é essencial para a criação bem-sucedida de políticas.

- **Mapas de interdependência**: a Akamai fornece um mapa para visualizar comunicações internamente e entre data centers de todos os tipos de tecnologias, como VMs, K8s, contêineres Docker e muito mais. Esses mapas permitem a visibilidade e a detecção de qualquer conexão suspeita entre pods, serviços e hosts ou namespaces.
- **Rótulos**: os mapas refletem com precisão a maneira como as aplicações são implantadas no cluster usando várias camadas de rótulos. Essa visualização descreve a hierarquia do K8s conforme planejada pelos gerentes da aplicação. Esse nível de detalhamento ajuda os usuários da Akamai a entender exatamente o que é implantado no cluster e as relações de rede entre as aplicações implantadas e o restante da infraestrutura.



Clusters representados no mapa de Exibição. Clicar duas vezes em um cluster exibe os namespaces e suas interconexões dentro do cluster.



O mapa de Exibição mostra informações de pods

> 93% dos entrevistados sofreram pelo menos um incidente de segurança em seus ambientes do K8s nos últimos 12 meses, às vezes levando a perda de clientes ou receita.

Execução. Para ajudar a minimizar a superfície de ataque em clusters do K8s, é necessária uma política de segmentação rigorosa. Uma solução de imposição de segmentação deve atender a dois critérios principais: ser não invasiva, sem qualquer limitação de escala e desempenho; e fornecer uma maneira flexível de delimitar todos os níveis de objetos do K8s, incluindo namespaces, controladores e rótulos do K8s.

A Akamai aproveita a CNI (Interface de Rede de Contêineres) nativa do Kubernetes. A CNI consiste em um plug-in de políticas de segurança de rede originalmente projetado para a imposição de segmentação de rede no K8s. É um método não invasivo sem limitações de escala. Os modelos dedicados permitem que os usuários protejam aplicações do Kubernetes fundamentais para os negócios, seja um namespace, uma aplicação ou qualquer outro objeto.

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

Modelo de proteção de aplicações do Kubernetes

Monitoramento avançado. Usando um sistema avançado de registro e monitoramento, um log de rede dedicado é configurado para redes do K8s, exibindo serviços de destino, IPs de nós, portas de origem e destino e os processos de cada evento. Isso fornece uma maneira fácil de investigar atividades anormais na rede e exportar dados para uma aplicação externa, como SIEM.

Resumo

O Kubernetes se tornou parte integrante de muitos ambientes corporativos. É uma abordagem diferente do que já vimos, oferecendo eficiência no uso de recursos, processos de desenvolvimento mais simplificados e maior portabilidade e escalabilidade. Mas essa abordagem diferente de desenvolvimento de aplicações também requer uma abordagem diferente de segurança.

A Akamai Guardicore Segmentation oferece uma solução holística que permite que você veja fluxos de comunicação entre diferentes tipos de implantações (bare-metal, VMs, K8s etc.), tudo a partir de um mapa. Ela fornece uma abordagem não intrusiva, escalável e nativa do K8s para fins de visibilidade, monitoramento e imposição que elimina a carga das equipes de segurança e desenvolvimento, permitindo que sua empresa inove rapidamente sem sacrificar a segurança.

De acordo com o Relatório de segurança State of Kubernetes da Red Hat de 2022, a segurança é uma das maiores preocupações com a adoção do K8s, e os problemas de segurança continuam causando atrasos na produção de aplicações.

Para saber mais, acesse akamai.com ou entre em contato com a equipe de vendas da Akamai.

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