Akamai

WHITE PAPER

Como atender às expectativas da conteinerização

Simplificando e acelerando a segmentação para ativos e aplicações críticos

Introdução

A conteinerização surgiu rapidamente como a solução preferida para a implantação de aplicações em ambientes de nuvem e híbridos, e a proliferação de contêineres continua a acelerar. De acordo com a Gartner, 90% das organizações globais executarão aplicações em contêineres em produção até 2026, um aumento de 40% em relação a 2021.[1] E, de acordo com um estudo da Forrester para Capital One, **86% dos líderes de TI pesquisados priorizaram o uso expandido de contêineres para mais aplicações**.[2]

> De acordo com o Gartner, até 2026, **90% das organizações globais** terão aplicações conteinerizadas em produção, em comparação a 40% em 2021

Tudo isso, é claro, coloca maior pressão sobre os responsáveis por proteger os ambientes de TI para acompanhar a implantação de contêineres, especialmente em um modelo DevOps que prioriza a rápida adoção e expansão. Embora várias soluções especializadas de segurança de contêineres tenham surgido, essas entidades específicas de plataforma, somente de contêineres, acabam adicionando complexidade e sobrecarga de gerenciamento sem abordar o data center corporativo como um todo, tornando a vida mais complicada para as equipes de segurança. O que é necessário é uma solução de segurança única e abrangente que funcione de forma consistente em todas as aplicações e tecnologias executadas em ambientes locais, de nuvem e híbridos, incluindo contêineres.

Antes de nos aprofundarmos em soluções, vamos dar uma olhada rápida no fenômeno de contêiner, nas forças que o impulsionam e nas implicações de uma perspectiva de segurança.

A pressão existe: As demandas de negócios impulsionam a adoção

O movimento em direção aos contêineres e seu crescimento projetado na adoção podem ser rastreados até as demandas de negócios que estão sendo cobradas nos departamentos de TI da empresa. As empresas modernas esperam poder se mover com velocidade e agilidade em resposta a ameaças competitivas e oportunidades de mercado. Elas precisam de soluções que apoiem a inovação e acelerem o tempo de lançamento no mercado. E estão sempre à procura de melhoria contínua da eficiência. Em um mundo cada vez mais interconectado, elas querem facilitar a realização de negócios digitalmente, com fornecedores, parceiros de negócios e especialmente seus clientes.

Esses são os principais motivos pelos quais a TI corporativa está migrando para a nuvem, ou mais precisamente para modelos híbridos no local/na nuvem. Eles também são os principais impulsionadores por trás da tendência de DevOps, que busca acelerar a implantação de aplicações críticas eliminando pontos de atrito, desde ideias até a implementação, aproveitando a automação e o escalonamento automático para colocar as aplicações em produção mais rapidamente.

> "As organizações muitas vezes subestimam o esforço necessário para operar contêineres na produção."
>
> — Gartner

Tudo isso ajuda a explicar por que os departamentos de TI adotaram a conteinerização. Em comparação com as máquinas virtuais, os contêineres são muito mais fáceis e rápidos de iniciar, permitindo a entrega em tempo real praticamente sem latência e permitindo que as equipes se concentrem em "aquecer os serviços, não os servidores". Uma das principais vantagens dos contêineres é a portabilidade para os ambientes de data center dinâmicos atuais; eles facilitam a migração de aplicações entre instalações locais para instâncias multinuvem. Isso é ainda mais aprimorado por meio da orquestração de contêineres via Kubernetes, ou "k8s", que permite que as equipes implantem e gerenciem volumes mais altos de aplicações em contêineres em escala em vários ambientes. A orquestração é cada vez mais considerada uma prática recomendada na implementação e no gerenciamento de contêineres.

Em resumo, os contêineres permitem que a TI responda melhor às demandas de negócios por velocidade, automação, resiliência e disponibilidade, e faça isso a um custo total de propriedade mais baixo em comparação com outras tecnologias. Os esforços de implementação, no entanto, não estão sem desvantagens. "As organizações muitas vezes subestimam o esforço necessário para operar contêineres em produção", diz um relatório da Gartner de 2019 sobre as práticas recomendadas de conteinerização.[3] Apesar do apelo popular da conteinerização, a tecnologia ainda é um tanto incipiente e as práticas recomendadas para implantação segura não estão totalmente consolidadas. De acordo com o relatório State of Kubernetes Security 2022 da Red Hat, "a segurança é [ainda] uma das maiores preocupações com a adoção de contêineres, e os problemas de segurança continuam causando atrasos na implantação de aplicações na produção."[4] Claramente, as empresas não podem colher todas as vantagens potenciais dos contêineres sem uma estratégia de implementação que inclui necessariamente a segurança cibernética.

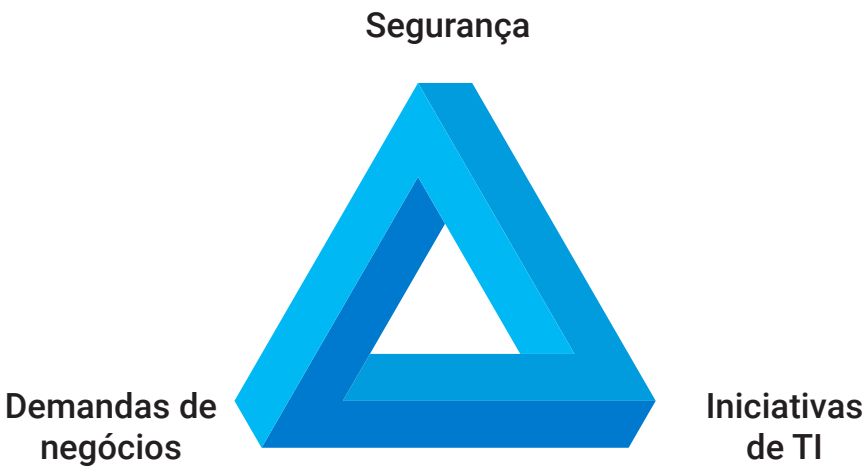
> De acordo com o relatório State of Kubernetes Security de 2022 da Red Hat, "**a segurança é [ainda] uma das maiores preocupações com a adoção de contêineres**, e os problemas de segurança continuam causando atrasos na implantação de aplicações para produção"

O que isso significa para a equipe de segurança?

"A segurança não pode ser uma reflexão tardia", afirma Gartner em seu relatório de práticas recomendadas. "Ela precisa ser incorporada ao processo de DevOps." No entanto, com demasiada frequência, não é isso que acontece. Na pressa de implementar a conteinerização, as equipes de segurança podem, por vezes, sentir-se no topo de um "triângulo impossível", uma ilusão de ótica também conhecida como o Triângulo de Penrose (também conhecido na Akamai como o Triângulo impossível de Klein e Howard).

> As soluções de segurança legadas não são adaptáveis à empresa moderna. As soluções de segurança devem ser rápidas, adaptáveis, dinâmicas e se encaixar perfeitamente em uma abordagem "DevSecOps".

Da mesma forma que o ponto mais alto do triângulo parece estar mais distante do que os outros dois cantos, a segurança parece ter ficado para trás em relação às demandas comerciais e das iniciativas de TI para atendê-las. Mas, assim como o triângulo é uma ilusão óptica, as soluções de segurança estão realmente mais próximas do que parecem. As equipes simplesmente precisam esquecer as soluções complexas e obsoletas que confiaram no passado e voltar o foco para soluções que mapeiem a maneira como a TI empresarial oferece hoje e que se encaixem perfeitamente em uma abordagem "DevSecOps". Isso significa uma solução rápida, adaptável e dinâmica e que, em si, emprega a abordagem do playbook DevOps. O mais importante é uma solução dissociada dos sistemas operacionais e da plataforma subjacentes para simplificar a implementação e o gerenciamento.



Triângulo Impossível de Klein e Howard

Por que "nativo" não é suficiente

No início da virtualização e migração para a nuvem, as empresas muitas vezes eram levadas a acreditar que os controles nativos da nuvem eram suficientes para visualizar, gerenciar e proteger suas cargas de trabalho. Somente depois de muitas tentativas e erros, os gerentes de TI perceberam que precisavam de um modelo de gerenciamento de sobreposição que incorporasse soluções de terceiros e oferecesse segurança que supere a dos controles nativos.

Como disse a Gartner e a Forrester Research, uma estratégia bem-sucedida de implementação de contêiner é baseada na "trifeta de contêiner"

- Execute contêineres de maneira portátil e independente de plataforma, que possa ser implementada em qualquer lugar em várias arquiteturas na nuvem e no local de maneira perfeita
- Aproveite a orquestração para executar e gerenciar contêineres em escala
- Use ferramentas de terceiros para gerenciamento de contêineres, visibilidade e segurança

Ao contrário dos esforços anteriores de virtualização e nuvem, o setor de contêineres reconheceu desde o início que os sistemas de gerenciamento nativos da nuvem e os controles de segurança especificamente são inadequados para uma estratégia de contêiner eficaz. No estudo da Gartner sobre soluções de gerenciamento de contêineres, **65% dos entrevistados disseram que pretendem utilizar ferramentas de gerenciamento de terceiros para visualizar, gerenciar e proteger cargas de trabalho em contêineres**.[5] No entanto, essas ferramentas de terceiros precisam trabalhar perfeitamente em instâncias locais e na nuvem e adotar uma abordagem granular para evitar as armadilhas de métodos complicados e mistos usados no passado como grupos de segurança, VLANs e firewalls, que oferecem visibilidade zero e granularidade insignificante.

Permita a adoção de contêineres com a Akamai Guardicore Segmentation

A Akamai Guardicore Segmentation foi projetada para atender aos desafios das atuais infraestruturas híbridas e dinâmicas de data center. Nós fornecemos visibilidade abrangente de todas as aplicações e cargas de trabalho em execução em vários ambientes e possibilitamos uma segmentação definida por software granular e facilmente implementada por meio da rápida criação, implementação e aplicação de políticas de segurança em aplicações individuais ou logicamente agrupadas.

Vamos deixar claro: a Akamai Guardicore Segmentation não é um produto pontual somente para contêineres. Em vez disso, a segurança de contêineres é um recurso-chave da plataforma, que funciona consistentemente em ambientes mistos que também podem incluir servidores bare-metal, máquinas virtuais, cargas de trabalho sem servidor e dispositivos remotos. Dessa forma, fornecemos às organizações uma solução única e abrangente para proteger todos os ativos de data center e nuvem, independentemente de onde residem ou de como são implantados, eliminando a necessidade de gerenciar várias soluções pontuais. E como nossa solução é dissociada das plataformas e sistemas operacionais subjacentes, as políticas de segurança seguem aplicações e cargas de trabalho à medida que se movem entre ambientes locais e em nuvem, aumentando o fator de portabilidade que torna os contêineres atraentes para a implantação de aplicações em infraestruturas de nuvem híbrida.

> A segurança de contêineres é um recurso fundamental da plataforma Akamai Guardicore Segmentation, que funciona consistentemente em ambientes de data center dinâmicos e heterogêneos

Com relação a contêineres, a Akamai Guardicore Segmentation funciona colocando agentes em nós de host de contêineres, permitindo a visibilidade de todo o cluster de contêineres, incluindo fluxos de comunicação de pod para pod e pod para máquina virtual. Isso permite a implementação e a aplicação de políticas de segurança muito granulares por processo, usuário e FQDN (Fully Qualified Domain Name, nome de domínio totalmente qualificado). Em um cenário de orquestração, oferecemos suporte à orquestração k8s e permitimos visibilidade dos metadados do Kubernetes e do OpenShift para um contexto superior. Um modelo de rotulagem flexível permite que os operadores expressem políticas usando a terminologia nativa do k8s. Para aplicação em k8s, aproveitamos a CNI (Container Network Interface) nativa, um método não invasivo para aplicar políticas em k8s 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. Também dimensionamos para k8s volumes de carga de trabalho e taxas de alteração. Como nossa solução também funciona em todas as outras cargas de trabalho empresariais de maneira semelhante, ela serve como uma única solução para visualizar, gerenciar e proteger ativos em toda a empresa.

De particular importância em um ambiente de DevOps, as políticas de segurança que você cria se integrarão de forma eficaz aos processos de integração contínua/implantação contínua (CI/CD), ajudando a garantir que a segurança não seja um pensamento secundário, mas totalmente integrada ao modelo de entrega.

Conclusão

Os contêineres são uma parte cada vez mais integral de muitos ambientes de negócios. Eles podem aumentar a eficiência do uso de recursos, simplificar processos e permitir maior portabilidade e escalabilidade. Ao mesmo tempo, a segurança integrada que eles fornecem não é suficiente, especialmente para empresas que utilizam um ambiente híbrido.

À medida que você procura uma solução de segurança que cresça com sua empresa, escolha uma ferramenta independente de plataforma que forneça percepções detalhadas sobre seus processos completos, independentemente de onde eles ocorram. A Akamai Guardicore Segmentation faz isso e muito mais, oferecendo a variedade de recursos e recursos que as empresas modernas precisam para estarem preparadas hoje e no futuro.

Usando a Akamai Guardicore Segmentation, sua equipe de segurança pode alcançar segurança consistente em ambientes de data center dinâmicos e heterogêneos. Ao fazer isso, você pode ajudar as equipes de TI a cumprir a promessa de conteinerização, realizando o desenvolvimento e a implantação rápidos, econômicos e seguros de aplicações essenciais para as demandas de negócios da sua empresa.

Simplifique a segurança em todo o seu ambiente. Saiba mais sobre nossa poderosa solução de segurança unificada para contêineres e muito mais: akamai.com/guardicore.

1 Chandrasekaran, Arun e Wataru Katsurashima. "The Innovation Leader's Guide to Navigating the Cloud-Native Container Ecosystem (guia do líder em inovação para navegar no ecossistema de contêineres nativos da nuvem)", Gartner, 18 de agosto de 2021.

2 "Adoção de contêiner de nuvem na empresa", Forrester, junho de 2020.

3 "Melhores práticas para execução de contêineres e Kubernetes em produção" , Gartner, 25 de fevereiro de 2019.

4 "Relatório de segurança do estado do Kubernetes", Red Hat, maio de 2022.

5 "Gartner prevê forte crescimento de receita para software e serviços globais de gerenciamento de contêineres até 2024", 25 de junho de 2020.

A Akamai protege sua experiência do cliente, sua força de trabalho, seus sistemas e seus dados ajudando a incorporar a segurança em tudo o que você criar, em qualquer lugar que você criar e entregar. A visibilidade da nossa plataforma em relação às ameaças globais nos ajuda a adaptar e desenvolver sua postura de segurança para permitir Zero Trust, interromper ransomware, proteger aplicações e APIs ou combater ataques DDoS, dando a você a confiança para inovar, expandir e transformar continuamente o que é possível. Saiba mais sobre as soluções de segurança, computação e entrega da Akamai em akamai.com e akamai.com/blog ou Akamai Technologies no Twitter e LinkedIn. Publicado em 05/23.