Akamai

WHITE PAPER

Como proteger cargas de trabalho em ambientes híbridos e multinuvem

Como proteger cargas de trabalho em ambientes híbridos e multinuvem

Em busca de inovação, vantagens competitivas e eficiências, as empresas migraram para um modelo de infraestrutura de nuvem baseado em DevOps. Dessa forma, elas aumentaram a velocidade e a agilidade da TI corporativa de modo nunca visto antes. Muitas organizações continuam a adotar infraestrutura de nuvem pública e novas abordagens de implantação, como contêineres e tecnologias sem servidor. Ao adotar esse novo modelo, a mais recente tecnologia de computação em nuvem está acelerando consideravelmente o ritmo da mudança. Essas práticas permitem que cargas de trabalho, aplicações e até mesmo ambientes sejam automatizados, dimensionados automaticamente, migrados e muito mais. As vantagens competitivas resultantes são poderosas.

Ao mesmo tempo, alguns serviços e sistemas legados, como infraestrutura tradicional de data center, permanecem em uso. As empresas podem estar no processo de removê-los ou modernizá-los, mas os sistemas inerentemente ainda existem porque contêm aplicações e fluxos de trabalho essenciais para os negócios.

Além disso, as técnicas de segurança tradicionais não conseguiram acompanhar o ritmo das mudanças, o que abre a questão de como proteger cargas de trabalho em nuvem nesses novos ambientes de nuvem híbrida e multinuvem. Além da velocidade, a segurança baseada em perímetro não é mais eficaz quando a grande maioria do tráfego ocorre dentro da nuvem ou do data center (leste-oeste) em vez de vir de fora (norte-sul). Essa transformação também força os executivos de TI a repensar seu manual de segurança.

As técnicas de segurança tradicionais não são eficazes em ambientes híbridos e multinuvem

Na verdade, nenhum modelo tradicional de segurança cibernética foi criado com a IaaS (infraestrutura como serviço) em mente. A nuvem pública precisa de novas estratégias baseadas em seus próprios desafios exclusivos.

A segurança corporativa deve evoluir para suportar o novo ambiente de negócios. As organizações já fizeram mudanças drásticas para atender aos requisitos de negócios e a metodologia de trabalho ágil. A segurança foi deixada para trás, apesar do investimento maciço realizado.

A realidade é que gastar dinheiro com soluções que foram desenvolvidas sem a nuvem em mente é um erro. Isso não ajuda a detectar e impedir violações atuais ou futuras. Então, como você pode consumir serviços de nuvem pública e aproveitar os benefícios de velocidade e agilidade, sem comprometer a proteção de dados essenciais?

O moderno data center de nuvem híbrida

A composição do data center moderno, a maior granularidade das cargas de trabalho e a velocidade do desenvolvimento estão mudando rapidamente. Um data center híbrido moderno típico é composto por cargas de trabalho executadas no local e na nuvem pública/IaaS, usando vários fornecedores e PaaS (plataforma como serviço) no local ou na nuvem. A quantidade de cargas de trabalho em execução na nuvem pública continua a crescer. Simultaneamente, os data centers locais não irão a lugar nenhum tão cedo. Caso em questão: uma pesquisa recente com executivos de tecnologia mostrou que, quando se trata de ambientes de TI modernos, cerca de 59% têm "alguns na nuvem, mas a maioria no local", com 34% tendo "principalmente na nuvem, mas alguns no local". Apenas 7% é "totalmente na nuvem", mas é esperado que esse número aumente drasticamente.[1]

Como podemos ver, as empresas estão cada vez mais adotando práticas de DevOps e melhorando sua agilidade. Os serviços de nuvem nativa e a tecnologia sem servidor estão se tornando mais fáceis de implementar. Ao usar uma combinação de contêineres, VMs e cargas de trabalho sem servidor na nuvem, você pode ser mais econômico e transformador do ponto de vista estratégico.

A segurança precisa se encaixar nesse paradigma de nuvem híbrida. As empresas precisam lidar com a segurança em cada estágio do processo de DevOps, desde testes, criação e planejamento até monitoramento, operação, implantação e lançamento de novos recursos. Migrar para a nuvem não pode ser um obstáculo que impeça o sucesso.

As cargas de trabalho distribuídas não estão bem protegidas, limitando o uso da nova tecnologia de nuvem

Atualmente, muitas empresas têm que proteger cargas de trabalho distribuídas no local, em locais compartilhados e em várias plataformas de nuvem pública/IaaS. Elas estão se esforçando para manter essas cargas de trabalho seguras com modelos tradicionais de segurança de rede local.

As questões são mais desafiadoras quando você tenta implantar novas ferramentas e técnicas baseadas em nuvem para proteger as novas tecnologias de nuvem. Os níveis de complexidade se multiplicam, à medida que as empresas tentam impor diferentes controles de segurança em diferentes ambientes e introduzir riscos implantando esses controles sem visibilidade adequada.

Em outras palavras, a nuvem, que é destinada a tornar as empresas mais dinâmicas, ágeis, rápidas e inovadoras, está colocando muitas organizações em risco. Com a falta de ferramentas de segurança relevantes focadas na nuvem, as empresas ficam limitadas em sua capacidade de adotar essa nova tecnologia sem causar pontos cegos e mais desafios.

É aí que entra a proteção adaptável da carga de trabalho.

A mudança para IaaS impulsiona a necessidade de proteção adaptável da carga de trabalho

A melhor maneira de proteger cargas de trabalho granulares com ciclos de vida curtos é com a aplicação dinâmica de proteção assim que a carga de trabalho estiver em uso. As soluções centradas na carga de trabalho são muito mais simples para aplicar a política de segurança do que os modelos tradicionais de segurança de rede quando se trata de infraestrutura de nuvem pública.

As plataformas de proteção da carga de trabalho na nuvem suportam soluções de segurança independentes de plataforma e centradas na carga de trabalho

Como uma política segue a carga de trabalho, independentemente da infraestrutura subjacente, o modelo pode ser aplicado a todas as cargas de trabalho em todo o ambiente de data center de nuvem híbrida. O resultado é uma abordagem consistente e independente de plataforma para controles de segurança.

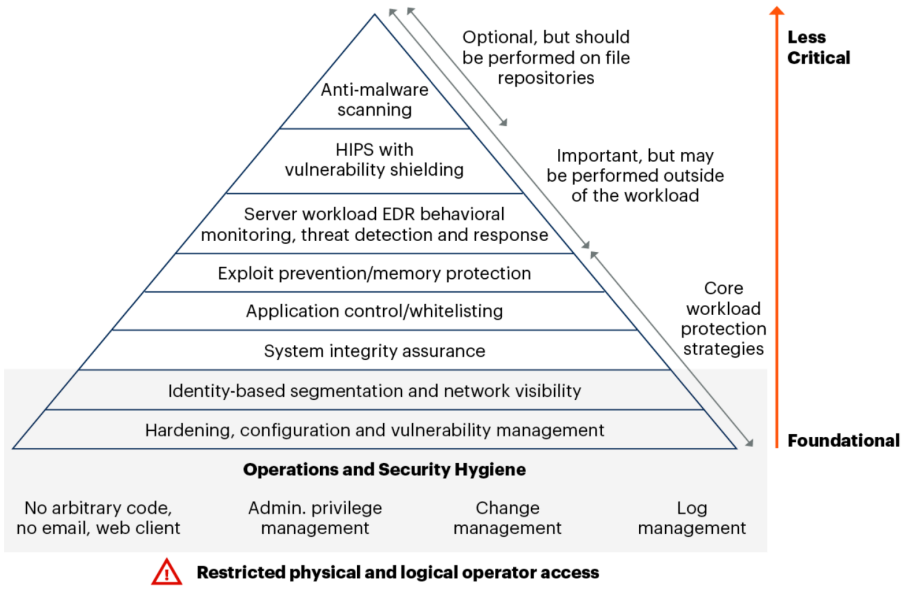
Embora existam ferramentas de segurança de nuvem nativas, as CWPPs (plataformas de proteção de carga de trabalho na nuvem) adaptáveis fornecem um controle mais abrangente e granular nos níveis de nome de domínio do processo, do usuário e totalmente qualificado. Elas também funcionam em vários provedores de nuvem e no local, fornecendo proteção mais forte e abrangente para VMs, contêineres e cargas de trabalho sem servidor.

Estratégias práticas de proteção de carga de trabalho principal: mapear controles para as diretrizes de proteção da carga de trabalho na nuvem da Gartner

Uma das diretrizes mais seguidas para proteção de carga de trabalho na nuvem foi escrita pelos especialistas do setor na Gartner. De acordo com a Gartner, há uma clara hierarquia de controles ao proteger cargas de trabalho na nuvem.

A pirâmide abaixo muda de fundamental para menos crítica, mostrando as estratégias que a Gartner considera fundamentais, bem como aquelas que são importantes, mas opcionais. Se possível, essas etapas devem ser incluídas em cada carga de trabalho, garantindo que a segurança seja integrada para cada ação na nuvem.

Hierarquia baseada em riscos dos controles de proteção da carga de trabalho[2]



As diretrizes de proteção da carga de trabalho em nuvem da Gartner fornecem uma hierarquia clara de controles de segurança para empresas

Veja, abaixo, uma explicação expandida das principais estratégias que nossa solução satisfaz para ajudar você a descobrir a melhor forma de incorporar essas estratégias no seu programa de proteção de data center híbrido ou multinuvem:

- **Fortalecimento, configuração e gerenciamento de vulnerabilidades**
  De acordo com a Gartner, a estratégia de proteção de carga de trabalho mais fundamental é configurar seus sistemas e configurações adequadamente para reduzir riscos. As ferramentas de gerenciamento de vulnerabilidades levam a remoção manual de vetores de ataque muito além e automatizam esse processo. Você pode então encontrar e resolver problemas de software que podem abrir portas para intenções maliciosas.

- **Segmentação baseada em identidade e visibilidade da rede**
  A Gartner destaca a segmentação e a visibilidade da rede como as principais estratégias para proteção na nuvem. A maioria das organizações está usando firewalls de última geração no local, mas muitas aceitam uma solução menos segura quando migram para a nuvem.

  As equipes de segurança entendem que os firewalls da próxima geração são insuficientes para a proteção na nuvem, mas não sabem como obter percepções ou controle heterogêneos em um ambiente de data center híbrido dinâmico. Então, vamos tirar um momento para ver como fazer isso direito.

  Primeiro, estabeleça a visibilidade. A visibilidade rápida resulta em menor tempo de retorno do investimento, pois todas as partes interessadas estão imediata e automaticamente alinhadas.

  As ferramentas nativas de nuvem podem fornecer mapas instantâneos ou registros textuais, mas geralmente são densas, incompletas ou insuficientes. A melhor solução deve descobrir automaticamente todas as aplicações, tráfego e dependências em sua rede. Dessa forma, você pode ver rapidamente todo o seu ecossistema de TI, mesmo quando sua empresa está distribuída de maneira híbrida.

  Sua solução também deve incluir um contexto eficiente, com forte percepção da imagem real do que está acontecendo no seu data center. Para qualquer empresa que esteja buscando gerenciar operações de segurança e consultas em escala, cada fluxo precisa ter esse contexto, com a capacidade de detalhar as comunicações individuais de processos e servidores. Isso permite o tipo de tomada de decisão baseada em dados que reforça a criação de políticas.

  Depois de estabelecer a visibilidade e o contexto, crie regras de segmentação que se ajustem às melhores práticas para o seu negócio. Por exemplo, você pode querer separar os ambientes de produção e desenvolvimento ou isolar os dados do cliente para comprovar a conformidade. Você também pode desenvolver políticas de microssegmentação mais granulares para fornecer segurança e controle profundos de uma forma que se adapte ao seu contexto de negócios específico.

- **Controle de aplicações/lista de permissões**
  Quando sua equipe de segurança pode definir políticas e ter certeza de que elas serão executadas em qualquer lugar, sua transição para a nuvem se torna mais simples e segura em todas as etapas.

  Confiar apenas em portas/IPs não dará o nível de visibilidade de que você precisa para proteção total da carga de trabalho na nuvem. O controle rígido do tráfego entre os componentes da aplicação é uma parte fundamental de uma solução de microssegmentação forte. As melhores tecnologias têm visibilidade e controle granulares, até o processo da aplicação, usuário e nome de domínio totalmente qualificado, usando detalhes como valores de hash, soma de verificação, caminho completo, resoluções e autenticações de armazenamento de identidade.

  Alguns recursos adicionais que podem aumentar o controle de aplicações incluem:

  - Microssegmentação que pode limitar o movimento lateral na nuvem, mesmo dentro do mesmo cluster de aplicações
  - Uma única abordagem de painel transparente, que se traduz em melhor segurança
  - A capacidade de criar modelos de lista de permissões e listas de proibições, os quais podem impedir aplicações ou tráfego não autorizados e garantir que conexões importantes sejam executadas sem impedimentos

- **Prevenção contra exploits/proteção da memória**
  A última estratégia de proteção de servidor principal no guia da Gartner para CWPP é a prevenção contra exploits. Procure uma ferramenta de segurança de microssegmentação que forneça detecção e resposta a violações. Dessa forma, você pode substituir ferramentas redundantes e reduzir a complexidade no seu data center.

  Além disso, como mencionado anteriormente, a visibilidade e o mapeamento são fundamentais. Depois de ter um mapa completo de toda a sua rede, é fácil ver vulnerabilidades não corrigidas ou comunicações maliciosas que estão agindo fora do normal. Quando sua empresa estabelece uma linha de base para tráfego legítimo, o movimento não sancionado se destaca.

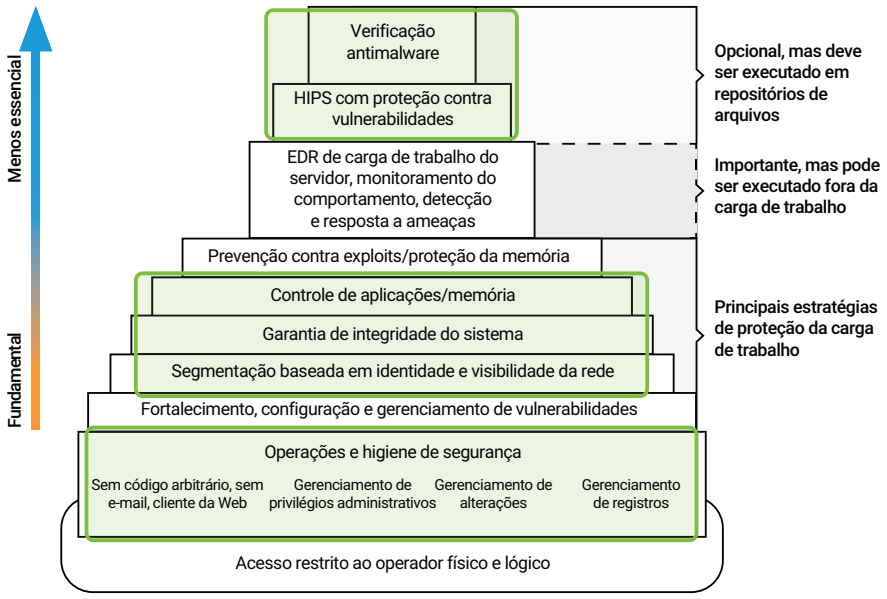
Outras estratégias importantes de proteção

As principais estratégias de servidor mencionadas acima são fundamentais para a segurança na nuvem. Ao mesmo tempo, a Gartner identifica várias outras estratégias que podem fortalecer seu ambiente híbrido ou multinuvem, incluindo EDR (detecção e resposta de endpoints) de carga de trabalho do servidor, monitoramento comportamental e TDR (detecção e resposta a ameaças).

EDR, monitoramento comportamental e TDR são partes importantes da detecção de violação e da resposta a incidentes. Para cobrir esses aspectos de segurança, procure uma solução que inclua análise de reputação. Isso permitirá que você identifique mais informações sobre um ataque, além de fornecer recursos avançados de fraude para induzir os invasores a divulgar seus métodos. Dessa forma, você pode fortalecer sua política e o procedimento de segurança daqui para frente.

Dados de visibilidade podem ser necessários para estabelecer informações sobre um evento anterior. Os melhores provedores armazenam seus dados por meses, permitindo que os usuários se concentrem em aplicações, processos e períodos específicos. As equipes de segurança também podem usar esses dados para investigação forense e melhoria da resposta a incidentes.

Akamai Guardicore Segmentation: protegendo cargas de trabalho de nuvem híbrida na hierarquia da CWPP



As áreas destacadas mostram onde nossa solução atende aos requisitos da CWPP

A Akamai Guardicore Segmentation aborda as lacunas inerentes às ferramentas nativas de segurança na nuvem, satisfazendo muitos dos princípios fundamentais estabelecidos na CWPP. Além disso, a solução oferece suporte inteligente à visibilidade, criação e aplicação de políticas em data centers híbridos e multinuvem.

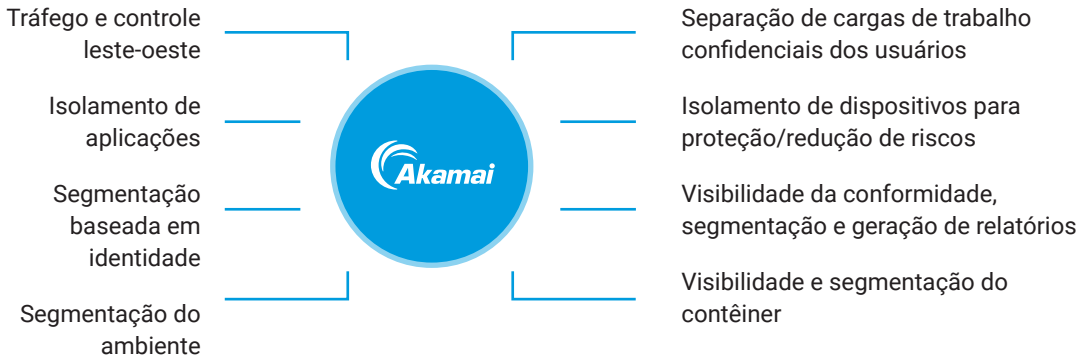
Nossa solução oferece visibilidade detalhada: um painel único que oferece uma visão de todo o data center. Ao visualizar seu data center híbrido como um todo, você pode entender completamente as dependências da aplicação e o efeito que qualquer política terá em sua rede. Isso tem um efeito poderoso na migração para a nuvem, levando os clientes à nuvem significativamente mais rápido do que as ferramentas nativas de visualização.

Essa visibilidade detalhada permite que você:

- Crie uma lista de tarefas para redes na nuvem
- Detecte rapidamente aplicações em qualquer infraestrutura e dependências de aplicações (um recurso essencial para uma migração bem-sucedida)
- Entenda sua infraestrutura e os custos operacionais com antecedência
- Obtenha informações sobre a criação da melhor política para reduzir os riscos das fases de planejamento de migração
- Tome o caminho mais curto, simples e seguro para suas metas de negócios para a nuvem

A visibilidade detalhada e baseada em contexto da Akamai Guardicore Segmentation resulta em uma compreensão rápida e completa de seus ambientes

Nossa visibilidade abrangente também vem com contexto para cada comunicação e fluxo, permitindo que você reduza erros e a complexidade geral. Você pode agrupar e filtrar as informações para apoiar qualquer parte interessada que esteja lendo o mapa, fornecendo facilmente as informações exatas de que elas precisam. Essa visão baseada em contexto reduz a necessidade de fornecedores terceirizados e criadores de políticas, resultando em uma compreensão rápida de seus ambientes para que você possa criar, refinar ou corrigir as políticas aplicáveis.



Exemplos de casos de uso da Akamai Guardicore Segmentation

Outros recursos essenciais que nossa solução oferece incluem:

- Políticas no nível de processos e de serviços, que permitem uma segurança mais simples e eficaz ao lidar com protocolos dinâmicos, como FTP ou Spark
- Políticas de microssegmentação baseadas em identidade, que impõem conexões com base no usuário que cria a conexão
- Políticas totalmente qualificadas baseadas em nomes de domínio que permitem acessar recursos de escalonamento automático cujos endereços IP são dinâmicos
- O uso de tags de nuvem pública existentes como rótulos, simplificando a visualização do seu data center híbrido ou multinuvem
- Criação automática de políticas a partir do tráfego observado, para que você obtenha orientação rápida e especializada ao iniciar sua jornada de microssegmentação

Nossa solução é independente de plataforma e infraestrutura, gerenciando a visibilidade e a aplicação em toda a infraestrutura

Reduzir a complexidade é o objetivo final ao procurar proteger um data center híbrido. Em resposta a essa necessidade, a Akamai Guardicore Segmentation é independente de plataforma e infraestrutura, oferecendo uma visão de toda a aplicação e política que segue a carga de trabalho, independentemente de onde ela reside. Cada regra é aplicada a todas as cargas de trabalho, desde o vCenter e nuvens públicas (AWS, Azure, GCP) até servidores e contêineres bare-metal.

A redução da complexidade não apenas resulta em uma postura de segurança mais forte, mas também alivia a carga de trabalho da TI e da segurança. Com grupos de segurança baseados em nuvem, você precisa de especialistas em nuvem nativa para cada fornecedor. Em contraste, com uma solução de segurança que gerencia a visibilidade e a aplicação em toda a infraestrutura, você só precisa de usuários certificados para uma única tecnologia.

Uma plataforma de proteção de carga de trabalho em nuvem preparada para o futuro

Um dos pilares da metodologia Agile e do DevOps é a capacidade de falhar rapidamente e passar facilmente para a "próxima grande novidade". Infelizmente, e ironicamente, a migração de suas cargas de trabalho entre diferentes provedores de nuvem pode deixar você extremamente lento. Também pode ser difícil fazer com a segurança mantida no local.

Você precisa ser capaz de manter suas opções abertas. Se você deseja mudar para uma infraestrutura multinuvem, ou até mesmo migrar cargas de trabalho para um novo provedor de nuvem, isso não deve ter um efeito negativo na segurança, nem a segurança deve impedir você de fazer a mudança.

A Akamai Guardicore Segmentation permite que você permaneça flexível e se mova no ritmo dos negócios, migrando suas cargas de trabalho com políticas de segurança intactas. Ela não atrapalha o processo ou a agilidade do DevOps, nem exige reconfiguração em todas as etapas. Em vez disso, ela fornece os fundamentos de uma plataforma confiável de proteção de carga de trabalho em nuvem, para que você possa manter seu data center híbrido ou multinuvem em segurança.

A Akamai Guardicore Segmentation permite a migração segura para a nuvem e entre nuvens, além de oferecer visibilidade inigualável com contexto. Com nossa solução, você pode aplicar a política até o nível do processo e do usuário e seguir suas cargas de trabalho onde quer que elas estejam.

Agora você pode tornar a segurança um recurso de todas as etapas do processo DevOps, proporcionando agilidade e suporte ao seu negócio. Sua organização será capaz de adotar habilidades de nuvem de ponta, mantendo a segurança em seu núcleo.

Saiba mais sobre como proteger ambientes de nuvem com a microssegmentação líder do setor. Visite akamai.com/guardicore hoje mesmo.

1 2022. Estudo sobre computação em nuvem da Foundry (antiga IDG).

2 Guia de mercado para plataformas de proteção de carga de trabalho em nuvem; escrito pelos analistas da Gartner Neil MacDonald e Tom Crow; publicado em 14 de abril 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 cria, em qualquer lugar que você crie e entregue. 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 apps 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 siga a Akamai Technologies no Twitter e LinkedIn. Publicado em 05/23.