Akamai

WHITE PAPER

Firewalls sob uma nova perspectiva

O caso econômico convincente para a segmentação baseada em software

Resumo executivo

Por que as equipes de rede e segurança ainda dependem de firewalls legados para fazer a segmentação de rede interna? À medida que aplicações e segmentos protegidos por políticas proliferam, os dispositivos físicos de firewall estão se mostrando muito complexos, inflexíveis e simplesmente ineficazes para atender aos desafios de segurança dos ambientes de nuvem híbrida cada vez mais dinâmicos de hoje. E eles são muito mais caros do que as equipes podem imaginar. Deixando de lado o enorme custo inicial de firewalls e hardware, há muitos custos downstream significativos devido ao gerenciamento de projetos, mão de obra, manutenção e o risco muito real de exposição prolongada de ativos devido a longos tempos de implementação. Se as empresas modernas desejam colher os benefícios do DevOps ágil, da implantação rápida de aplicações e da nuvem, deve haver uma maneira melhor de proteger ativos essenciais com segmentação. Agora existe: segmentação baseada em software. É mais fácil, mais rápida, mais eficaz e, como este documento demonstrará claramente, oferece segurança ideal a um custo total de propriedade muito menor do que os métodos de segmentação tradicionais.

Introdução

Hoje, vemos três forças convergentes impulsionando a demanda por meios mais granulares de segmentação de redes e ativos individuais. Primeiro, o DevOps ágil e outros modelos de entrega rápida estão valorizando a implantação acelerada de aplicações na produção. Inevitavelmente, isso exige a criação de zonas mais seguras com políticas mais precisas. Em segundo lugar, à medida que as organizações migram para a nuvem e adotam infraestruturas de TI híbridas, suas aplicações geralmente migram entre diferentes ambientes, o que aumenta o tráfego entre segmentos em toda a rede. E, em terceiro lugar, a rápida proliferação de aplicações devido ao desenvolvimento ágil está criando uma superfície de ataque cada vez maior para os hackers.

Firewalls para segmentação: além de seu auge

Dadas essas condições, uma dependência estrita de VLANs e firewalls para fins de segmentação está se tornando insustentável. De uma perspectiva puramente técnica, a configuração de várias instalações de VLAN e firewall de uma forma que acompanhe o desenvolvimento da aplicação é complexa e incômoda. Também é trabalhosa, desviando muitos membros da equipe de projetos de segurança de alta prioridade. O tempo de implantação é outro problema, aumentando o risco de exposição e vulnerabilidade prolongada dos ativos. E, acima de tudo, é extremamente cara de implementar, não apenas devido ao custo inicial de firewalls e novo hardware para suportar tráfego adicional, mas também devido aos custos associados ao gerenciamento contínuo, a modificações e à manutenção das instalações.

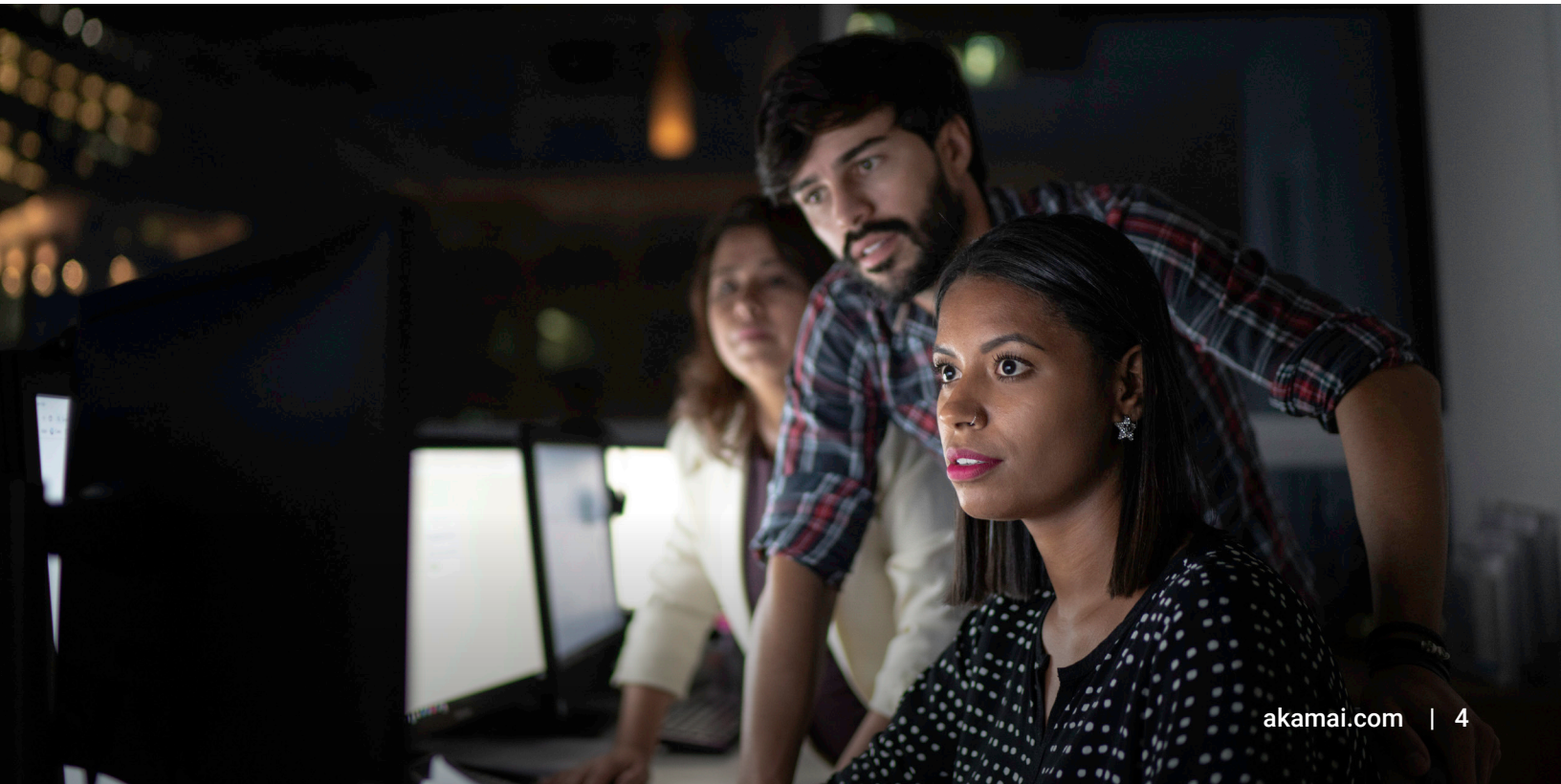
Em poucas palavras, as abordagens tradicionais de segmentação de rede atingiram um limite. Em particular, à medida que as organizações buscam tirar proveito da nuvem dinâmica e dos ambientes híbridos, a dependência de firewall interno para segurança limita sua agilidade, velocidade para criação e aplicação de políticas e capacidade de dimensionar com segurança suas operações. A necessidade de uma alternativa de segmentação moderna, simplificada, menos dispendiosa e mais eficaz para firewalls legados nunca foi tão urgente. Entre na segmentação baseada em software.

A necessidade de uma alternativa de segmentação moderna, simplificada, menos dispendiosa e mais eficaz para firewalls legados nunca foi tão urgente.

Sentir a dor: a cara tarefa de gerenciar firewalls

Antes de se aprofundar nas vantagens da segmentação baseada em software, convém contrastá-la com o status quo. À medida que uma empresa cresce, também cresce o número de aplicações e a quantidade de tráfego de dados associados, gerando demanda por segmentos de rede adicionais e políticas de segurança mais complexas. Se você depende de VLANs protegidas por firewall, cada nova implantada precisa ser adicionada a cada porta de switch trunk por meio da qual o tráfego entre segmentos flui. Uma sub-rede IP também precisa ser criada para cada nova VLAN. Uma subinterface também deve ser criada para o firewall. As políticas de firewall precisam ser criadas. Cada uma dessas alterações geralmente requer aprovações, janelas de manutenção e a possibilidade de tempo de inatividade, o que significa maior risco de interrupção da rede.

A adição de VLANs e firewalls envolve um processo doloroso de várias etapas envolvendo até cinco equipes, separadamente responsáveis por comutação, roteamento, implementação de firewall, servidores ESXi e criação de políticas de segurança. Tudo isso contribui para a duração da implementação, sujeita a organização a riscos prolongados e aumenta os custos de software, hardware e mão de obra. Além disso, do ponto de vista do engenheiro, esse é um trabalho de alto risco e baixa recompensa: ele exige muito esforço e oferece pouco proveito, desviando tempo e recursos de outras atividades de gerenciamento de risco de alta prioridade. Infelizmente, poucas das etapas no processo de gerenciamento de alterações dentro do ambiente de VLAN com firewall se prestam à automação.



Encontrar a cura: segmentação baseada em software em três etapas fáceis

A tecnologia de firewall de perímetro legado simplesmente nunca foi destinada às demandas mais precisas e restritas por largura de banda da segmentação interna granular. A segmentação baseada em software surgiu nos últimos anos como uma alternativa viável, mais rápida, mais eficaz e de menor custo para atender à demanda de segmentos de rede mais e mais rígidos nos ambientes dinâmicos atuais. O núcleo da implementação da segmentação baseada em software é o conceito de um "firewall distribuído" que seja muito mais ágil e fácil de gerenciar do que um dispositivo de firewall de rede tradicional.

A segmentação baseada em software torna possível uma implantação **10 ou até 20 vezes mais rápida** em comparação com o firewall tradicional, com necessidade de menos pessoas e praticamente nenhum tempo de inatividade ou interrupção.

Um exemplo líder do setor de uma solução de segmentação baseada em software é a Akamai Guardicore Segmentation. Em comparação com o processo demorado, caro e complexo de implementação de firewall de VLAN, nossa solução de segmentação baseada em software envolve apenas três etapas:

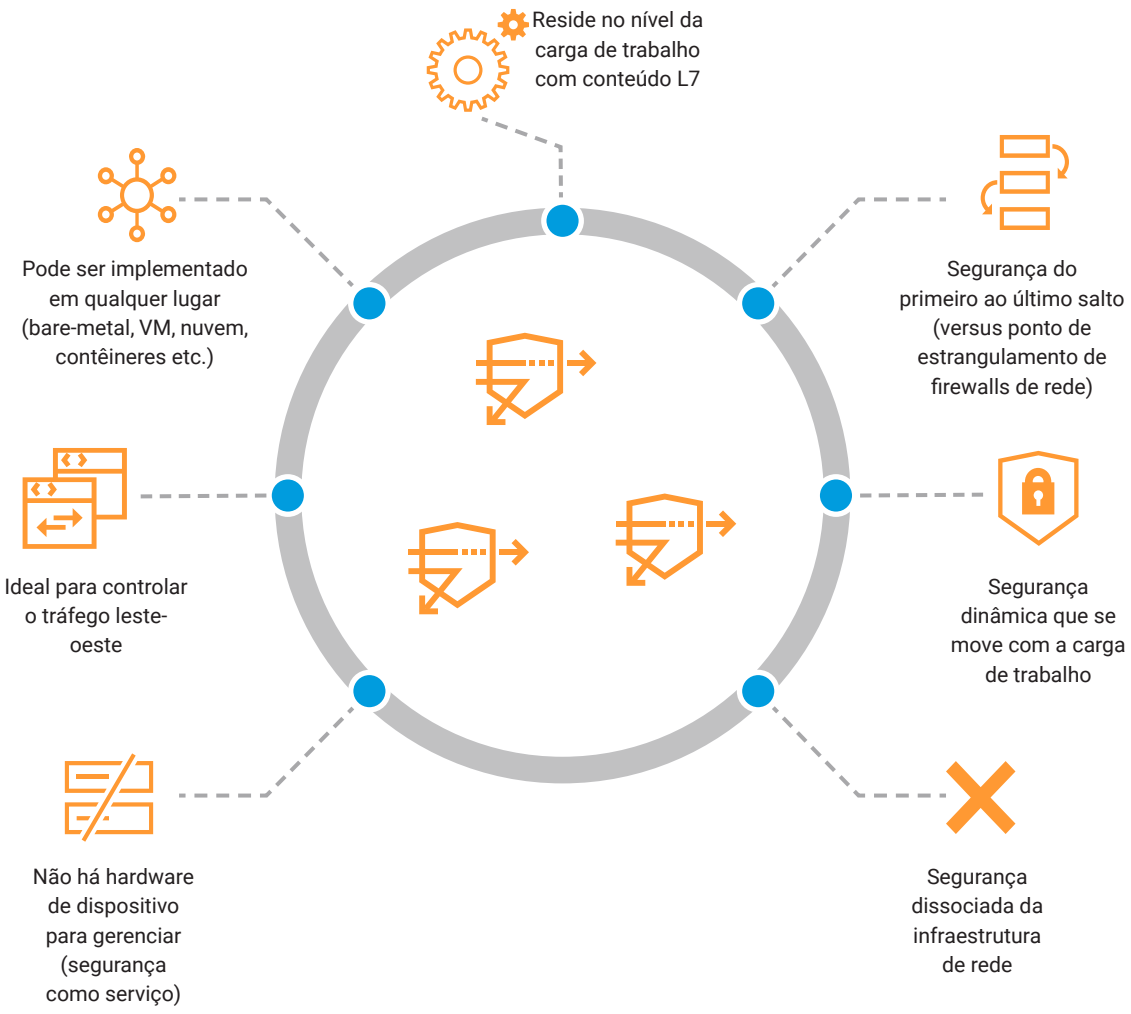
1. **Identificar e rotular os ativos:** uma grande barreira encontrada durante o processo tradicional de firewall é a falta de visibilidade dos ativos que precisam ser protegidos. A Akamai Guardicore Segmentation inclui um recurso de visualização que permite que os operadores identifiquem e rotulem todas as aplicações e suas dependências em execução em toda a infraestrutura de uma organização.

2. **Visualizar e agrupar por rótulo:** após obter a visibilidade contextual, os operadores podem organizar aplicações em grupos lógicos com base em seus rótulos e mapear as dependências entre eles. Nosso processo de rotulagem é muito flexível e permite que você agrupe aplicações com base em seu próprio contexto de negócios, usando a terminologia com a qual você já está familiarizado.

3. **Criar políticas:** os operadores podem então criar políticas de segurança granulares que determinam quais aplicações têm permissão para se comunicar umas com as outras com base nos fluxos reais observados. Modelos de política pré-criados para casos de uso comuns simplificam ainda mais o processo. Agora, aplicações e fluxos de trabalho são efetivamente segmentados uns dos outros, independentemente de onde estejam no ambiente.

A segmentação baseada em software é 10 ou até 20 vezes mais rápida de implantar em comparação com o firewall tradicional, com necessidade de menos pessoas e praticamente nenhum tempo de inatividade ou interrupção. Além disso, depois de iniciar o processo de visualização e segmentação, você pode facilmente dividir ainda mais sua rede ou adicionar diferentes políticas com base em rótulos, automatizar processos, abordar incidentes de segurança e fazer alterações rápidas em resposta a requisitos comerciais ou regulamentares.

Vantagens do firewall distribuído



Estudo de caso: grande processadora de alimentos economiza 85% na segmentação

Uma grande processadora de produtos suínos dos EUA precisava segmentar 45 aplicações com uma média de cinco servidores por aplicação, implantados em dois locais. O objetivo da empresa era eliminar suas redes planas, com o mínimo de interrupção do serviço, e implementar políticas o mais rápido possível.

Após uma análise das alternativas, a empresa escolheu a solução de segmentação baseada em software da Akamai. Embora a velocidade e a simplicidade da implementação tenham sido tomadas na decisão, o fator decisivo foi uma análise que mostrou uma economia de mais de US$ 900.000 (ou 85%) em um período de três anos, em comparação com a proteção de VLANs com um importante fornecedor de firewall. Em particular:

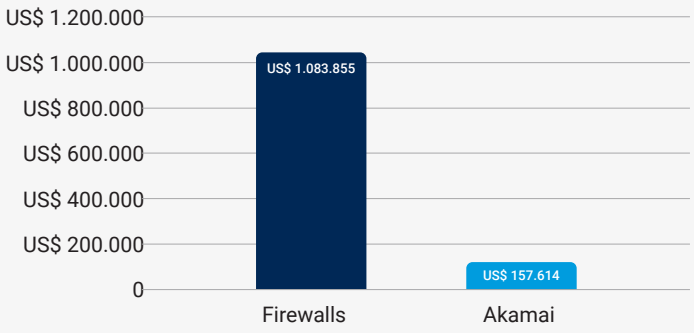
- O custo de licenciamento da Akamai Guardicore Segmentation foi 55% menor do que o custo de hardware para uma implementação de firewall de VLAN.
- O custo da mão de obra, com base na suposição de US$ 2.000 por semana, foi 93% menor com a Akamai do que com um projeto de VLAN com duração muito maior.

Além disso, a Akamai atendeu à necessidade do cliente de implementação rápida de políticas, garantindo 45 aplicações sem interrupção em apenas seis semanas.

TCO do firewall*
US$ 1.083.855

TCO da Akamai*
US$ 157.614
-US$ 926.241

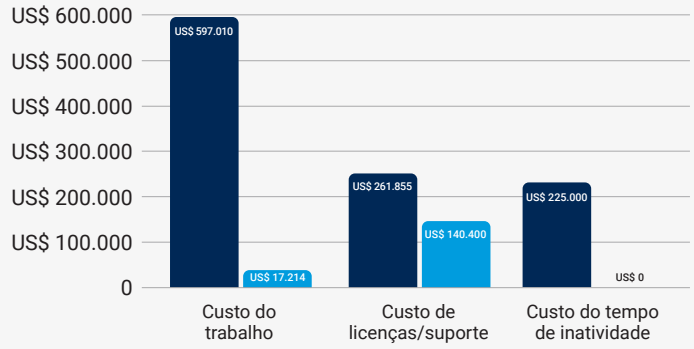
* Custo em um período de 3 anos



O custo do trabalho da Akamai*
US$ 17.214
-US$ 579.796

O custo de licenças/suporte da Akamai*
US$ 140.400
-US$ 121.455

O custo do tempo de inatividade da Akamai*
US$ 0
-US$ 255.000



O que tudo isso significa

A segmentação baseada em software oferece três vantagens principais em relação aos métodos tradicionais de firewall:

Redução de riscos mais eficaz: ao permitir a rápida segmentação de aplicações em um nível bastante granular, a segmentação baseada em software resulta em uma superfície de ataque amplamente reduzida. Aproveitando os princípios Zero Trust, (que exigem autenticação rigorosa de qualquer usuário, dispositivo ou aplicação que tente acessar um ativo de rede) a segmentação baseada em software impede o movimento lateral de ameaças dentro do data center ou ambiente de rede. Isso atenua ainda mais o impacto das violações de dados, tornando os invasores incapazes de assumir qualquer processo, mesmo que tenham rompido com sucesso as defesas do perímetro. Ela também permite que as empresas atinjam mais rapidamente a conformidade com os regulamentos que exigem o isolamento distinto de aplicações essenciais e confidenciais do tráfego geral da rede.

Velocidade para uma postura de segurança excelente: em resumo, a segmentação baseada em software torna você mais seguro e mais rápido, permitindo que as equipes de segurança acompanhem o ritmo da implantação ágil de aplicações DevOps e garantam que todas as aplicações em produção fiquem protegidas adequadamente. Isso também significa que menos recursos, técnicos ou humanos, são vinculados a projetos de segmentação por longos períodos. As equipes podem concentrar seu tempo em outras iniciativas importantes.

Reduza consideravelmente o custo total de propriedade: esse é o resultado real e, provavelmente, a vantagem mais significativa de uma perspectiva comercial. A segmentação baseada em software pode ser alcançada com muito menos CapEx (despesas de capital) para uma solução de software em comparação com a compra de dispositivos de firewall e hardware adicional. Isso também resulta em OpEx (despesas operacionais) muito mais baixas ao longo do tempo na forma de economia de mão de obra e recursos para manutenção e gerenciamento contínuos.

Somente com base nessas medidas, em uma comparação lado a lado entre a segmentação baseada em software e uma solução de firewall para 10 segmentos de aplicação, a abordagem da Akamai demonstrou oferecer uma economia potencial total de 85%, totalizando cerca de US$ 1 milhão.

É claro que, embora se possa esperar economias mensuráveis na primeira semana de implantação, o TCO (custo total de propriedade) significa muito mais do que apenas o preço inicial de compra ou os custos contínuos desembolsados. Embora as etiquetas de preço completas possam não estar facilmente aparentes, a segmentação baseada em software produz economias substanciais ao praticamente eliminar o tempo de inatividade e a interrupção do serviço. Além disso, as empresas evitarão perdas financeiras resultantes de violações de dados, bem como penalidades por descumprimento. Também reduzirão muito o risco de danos à reputação e perda de negócios após uma violação. Equipes e recursos de TI podem ser reimplantados longe do gerenciamento de alterações de firewall e voltados para projetos mais produtivos. Todos esses fatores de custo contribuem para um TCO mais baixo e uma margem de lucro maior para aqueles que optam por uma solução de segmentação baseada em software.

Estudo de caso: grande banco global, enfrentando sanções de conformidade, recorre à Akamai Guardicore Segmentation

Após uma auditoria que revelou riscos de segurança em suas redes planas e diante de um conjunto de novas regulamentações que exigem uma segmentação mais rigorosa, uma importante instituição financeira europeia iniciou um projeto de segmentação usando VLANs e regras de firewall. Este projeto estava tomando um tempo considerável, exigindo várias partes interessadas e equipes, causando paradas de produção e ambiguidades de políticas. Como resultado, o banco estava pagando multas por descumprimento, além de custos de implementação insustentavelmente altos.

A equipe de TI procurou rapidamente por soluções alternativas e ficou impressionada com o nível de automação que a Akamai poderia trazer para suas operações de segurança. O banco implantou a Akamai Guardicore Segmentation em várias regiões e tipos de infraestrutura de TI. O projeto levou menos de três meses, 10 vezes mais rápido do que inicialmente estimado com métodos tradicionais de segmentação. O banco não só atualizou sua postura de segurança, mas também atendeu aos requisitos de conformidade para mais de 10.000 ativos.
A implantação rápida resultou em redução acelerada de riscos, juntamente com uma economia considerável de custos e recursos internos.

Grande banco global

Meta do projeto:

Desenv/Prod/Separação de UAT

Escopo do projeto:

1. Restringir o tráfego entre ambientes de produção e não produção
2. Prontidão do isolamento de aplicações

Segmentação legada

- Progresso extremamente lento
- Falhas de auditoria, multas e erros de produção
- Interrupções da produção devido ao tempo de inatividade da aplicação

Tempo: 2 anos com firewalls/VLANs

Impacto da Akamai

- 10.000 ativos não compatíveis segmentados
- Tempo de inatividade zero da aplicação
- Implementação 10 vezes mais rápida
- Esforço manual reduzido com DevOps

Tempo: 6 meses **Pessoas:** 3 arquitetos

Conclusão: tudo conta

Os firewalls não estão obsoletos. Eles certamente têm um papel a desempenhar na proteção do perímetro da rede. Mas nos ambientes dinâmicos atuais, o perímetro se tornou um conceito um pouco amorfo. Para alcançar o equilíbrio necessário entre segurança e agilidade, as organizações precisam ser capazes de proteger seus ativos digitais não apenas no nível de rede L4, mas também no nível de aplicação L7 (especificamente, processos individuais). E para esse propósito, os firewalls não são apenas inadequados, mas também atrapalham o progresso. A tentativa de segmentação granular com firewalls é um grande consumo de recursos, sejam humanos, técnicos e financeiros.

Quando comparada aos firewalls, a segmentação baseada em software demonstrou reduzir significativamente o risco de segurança e o tempo total de valorização com um TCO significativamente menor do que as abordagens tradicionais, o que se traduz em um ROI maior alcançado mais rapidamente. Essa não é uma visão futurista. A segmentação baseada em software chegou e está oferecendo esses benefícios para organizações em inúmeros setores neste momento.

Um estudo sobre a evolução da TI

A história da tecnologia é de melhoria constante, simplificação e redução de custos. A segmentação não é exceção.

Considere o exemplo do armazenamento, que em apenas duas décadas evoluiu de disquetes para unidades flash, depois NAS (armazenamento conectado à rede) e, por fim, armazenamento em nuvem. Ou tempo de execução de computação, que evoluiu de servidores para máquinas virtuais, computação em nuvem para contêineres e, por fim, para computação sem servidor. Em cada caso, os principais fatores foram economia de custos e maior flexibilidade. E, claro, os rápidos avanços na tecnologia tornaram isso possível.

A evolução da segmentação de dispositivos físicos de firewall para firewalls distribuídos baseados em software, abstraídos da rede, é semelhante. E os drivers subjacentes são os mesmos: custo reduzido e maior flexibilidade (que se traduz em velocidade de implantação), ao mesmo tempo em que melhora constantemente a eficácia das políticas de segurança com uma abordagem mais granular que suporta Zero Trust.

É hora de as equipes de rede e segurança adotarem um novo modelo de segurança com segmentação, como claramente fizeram em outros setores de tecnologia. O firewall físico para segmentação segue o caminho do disquete.

Quer ver nossa solução em ação?
Solicite uma demonstração hoje mesmo: akamai.com/guardicore