Akamai

WHITE PAPER

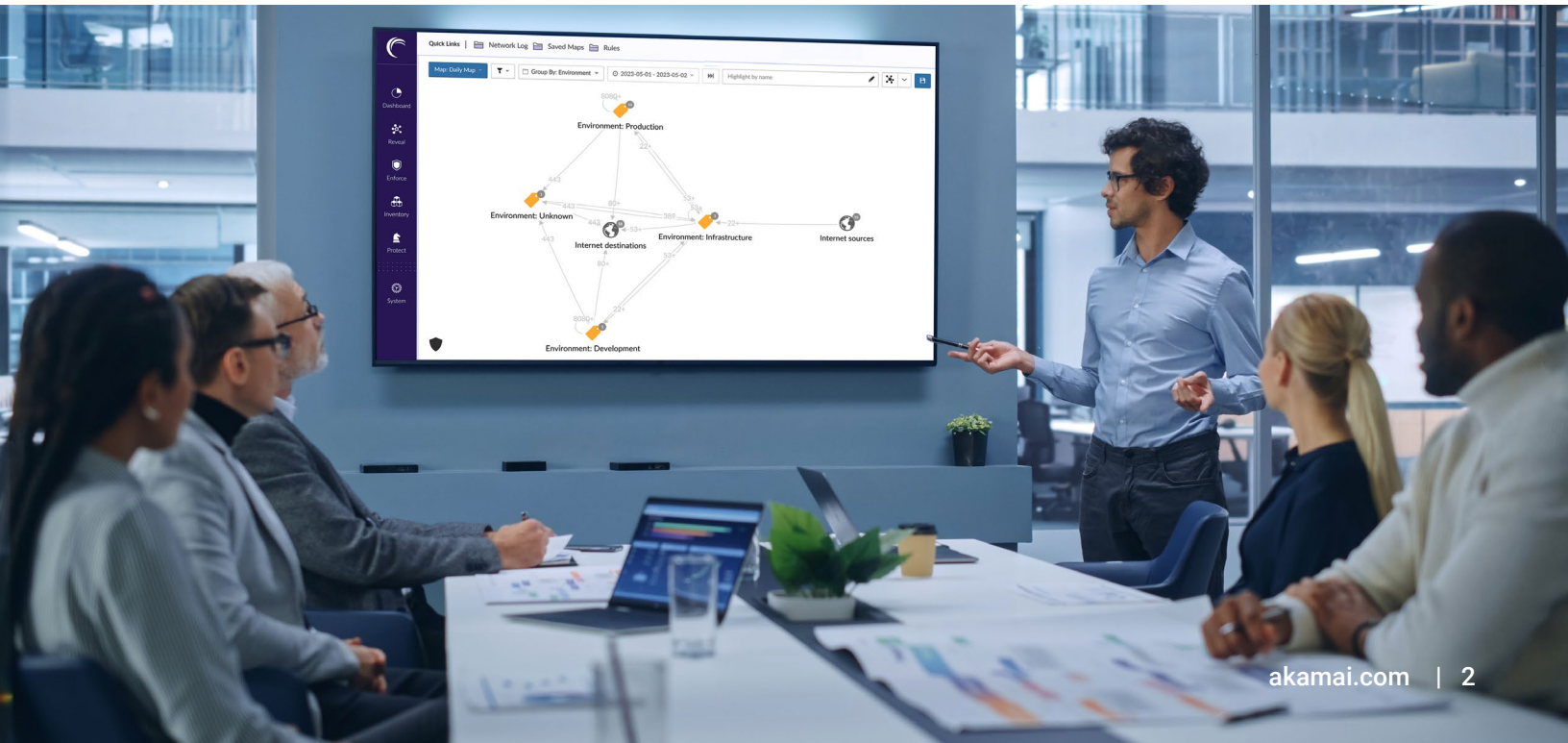
Segmentação definida por software para operadores de data center

Para os operadores de data centers multilocatários, a segmentação de ambientes de computação não é apenas importante. Ela é fundamental para o modelo operacional deles. Primeiro, eles precisam separar sua própria infraestrutura dos ambientes de seus clientes e compartilhar determinados recursos enquanto impedem o acesso a outros. Segundo, eles precisam evitar "contaminação cruzada" entre os respectivos ambientes de seus clientes, seja acidental ou nefasta. Isso inclui impedir que violações ou infecções por malware bem-sucedidas se espalhem do ambiente de um cliente para outros. Finalmente, dentro das aplicações operacionais próprias, um bom nível de separação é necessário para limitar o impacto de uma possível violação. Analisando mais profundamente as redes operacionais dos provedores de data center, existem três cenários em que a segmentação, se alcançada de forma eficiente, pode melhorar significativamente a postura de segurança e reduzir os custos.

1. **Separar redes operacionais** (DCIM, BMS etc.) da rede corporativa (os sistemas internos do provedor, que incluem faturamento) e redes de clientes

2. **Reduzir o risco de movimento lateral dentro da rede operacional**, que tem muitos sistemas de difícil aplicação de patches e introduz riscos se não forem segmentados adequadamente

3. **Criar conectividade eficiente e segura entre redes voltadas para o cliente**, como a DMZ, onde o portal personalizado está localizado, que precisa de acesso seguro aos dados de redes operacionais (leitura do status de energia, por exemplo) e de redes corporativas (para leitura das informações de cobrança)



Eles são tratados hoje por meio de construções de rede muito complexas, lentas de implementar e ineficientes, VLANs, redes provisórias etc. A implementação de uma solução definida por software sem depender de configurações de rede complexas terá reduções significativas de custos e também introduzirá um controle mais rígido e robusto da conectividade.

Além disso, os clientes se esforçam para implementar e manter um nível forte de segmentação em seus aplicativos (hospedados ou no local). Isso introduz uma importante oportunidade para os operadores de data center aproveitarem sua experiência de segmentação interna, ferramentas e modelos operacionais para oferecer serviços gerenciados a seus clientes e criar um fluxo de receita muito atraente em torno de uma prática de segmentação. Além disso, com a capacidade de estender as políticas de segurança às instalações do cliente com a metodologia, ferramentas e processos corretos o operador poderá obter acesso e visibilidade aos aplicativos não hospedados, o que pode ajudar a acelerar sua migração segura para o data center hospedado, contribuindo assim para os negócios principais.

Equifax: o pior cenário

Se você está se perguntando "o que de pior pode acontecer" com uma segmentação ambiental fraca, ineficaz ou inexistente, a altamente divulgada violação da Equifax em 2017 é um excelente exemplo histórico. A violação resultou no comprometimento de 143 milhões de informações pessoais altamente confidenciais dos americanos. De acordo com a investigação do GAO (Government Accountability Office, escritório de contabilidade do governo) dos EUA, os invasores inicialmente invadiram o portal de resolução de disputas de clientes da gigante agência de crédito explorando uma vulnerabilidade, conhecida como CVE 2017-5638, na estrutura da web Apache Struts. Uma vez lá dentro, eles basicamente tiveram acesso livre aos sistemas da empresa por 76 dias. O relatório do GAO atribuiu esta liberdade de movimento lateral à falta de segmentação, o que permitiu fácil acesso às bases de dados à vontade — um ataque praticamente ilimitado.

A questão é como conseguir esse tipo de segmentação de forma mais eficaz, eficiente e econômica. Historicamente, as operadoras contam com firewalls tradicionais ou VLANs para separar ambientes em uma arquitetura multilocatária ou multiusuário. A implementação e manutenção dessas medidas, no entanto, é geralmente árdua, altamente manual, demorada e cara. Além disso, essas técnicas não são, de forma alguma, herméticas e podem deixar uma quantidade substancial de superfície de ataque exposta. A eficácia das soluções projetadas para defesa de perímetro é particularmente problemática no data center, especialmente porque a maioria desses ambientes inclui uma variedade de máquinas virtuais, hipervisores, contêineres e até mesmo componentes de nuvem, e as cargas de trabalho giram dinamicamente para cima e para baixo automaticamente. Outra observação importante é que a segmentação com VLANs requer tempo de inatividade de um aplicativo, que para controles operacionais críticos pode ser um obstáculo.

Por todas essas razões, os operadores de ambientes compartilhados estão observando mais detalhadamente as técnicas modernas de segmentação definidas por software, incluindo a microssegmentação. Os avanços nas tecnologias de microssegmentação tornaram-na uma opção viável para todos os tipos de empresas e, provavelmente, a escolha ideal para alcançar um modelo de segurança Zero Trust. De igual importância, com as ferramentas certas e um pouco de planejamento cuidadoso, a microssegmentação pode ser implementada de forma mais rápida e fácil do que os métodos mencionados anteriormente, além de ser mais fácil de gerenciar e manter. Na verdade, testes recentes demonstraram que a microssegmentação pode reduzir o tempo de implantação em até 30 vezes em comparação com a implementação de firewall tradicional. Um benefício crucial adicional: Com a segmentação definida por software, não são necessárias alterações de rede ou tempo de inatividade do aplicativo. Essas economias de tempo e eficiências se traduzem em custos significativamente mais baixos ao longo do ciclo de vida da implantação.

As armadilhas das abordagens convencionais

Para entender as vantagens da segmentação definida por software ou da microssegmentação, é útil para fins comparativos examinar algumas das desvantagens e limitações das técnicas padrão empregadas no local e na nuvem. Isso pode incluir alguma combinação de firewalls físicos ou virtualizados e configurações de rede, como VLANs. Em geral, esses métodos exigem muitos recursos e mão de obra. Criar políticas de segurança é um processo complicado. Adições e modificações precisam ser realizadas manualmente, criando um obstáculo à eficiência operacional contínua e aumentando o risco de vulnerabilidade.

Os firewalls internos, em particular, são caros para adquirir e complexos para configurar. Eles também interferem no fluxo normal de tráfego, alterando padrões e criando "grampos" sinuosos que, por fim, impedem o desempenho do sistema. Como o setor está aprendendo, os firewalls não se destinam à segmentação dentro do data center, alguns provedores admitem prontamente que os firewalls simplesmente não pertencem a ele.

Um dos desafios mais difíceis ao tentar introduzir a segmentação em um ambiente de produção existente e em execução é que os métodos tradicionais exigem tempo de inatividade para um aplicativo. O tempo de inatividade é caro. Isso só pode acontecer dentro de janelas de tempo específicas e, muitas vezes, não é possível.

Um desafio adicional que vale a pena notar é que a criação de qualquer segmentação interna requer um bom conhecimento das dependências de aplicativos leste-oeste. Essa percepção geralmente não existe. Sem uma maneira simples de mapear dependências de aplicativos, é extremamente difícil e arriscado separar um ambiente brownfield.

Por que a segmentação definida por software é mais eficaz

Eficiência operacional, melhor postura de segurança: a segmentação definida por software supera as ineficiências inerentes das técnicas tradicionais e, talvez, mais importante, resulta em maior segurança para ambientes multiusuário. Como o nome sinaliza, a segmentação definida por software usa o conceito de segmentação de rede e o implementa sem qualquer necessidade de mudança de infraestrutura. Isso implica a criação de políticas de segurança em torno de aplicações individuais ou agrupadas logicamente, independentemente de onde residam no data center híbrido. Essas políticas determinam quais aplicativos podem ou não se comunicar entre si — o verdadeiro Zero Trust.

Sem alterações manuais ou tempo de inatividade: a segmentação definida por software não requer nenhuma alteração de rede ou nenhuma VLAN a ser criada, o que resulta em economias operacionais significativas. Ela também não requer nenhum tempo de inatividade ou alteração de aplicativo devido a uma migração para uma nova VLAN. Isso é importante. Em muitos aplicativos para os quais o tempo de inatividade é muito caro ou impossível, essa é a única maneira de fornecer essa medida de segurança crucial.

Ampla visibilidade: além disso, soluções avançadas de segmentação definida por software, projetadas para enfrentar os desafios de segmentação de tráfego leste-oeste, fornecem uma ferramenta de visibilidade integrada que ajuda a identificar os limites do segmento e as dependências do aplicativo. Isso resulta em um processo eficiente e elimina erros operacionais ao criar as políticas.

Automação de políticas e controles: a segmentação definida por software também possibilita a aplicação de políticas de forma dinâmica, de modo que, à medida que as cargas de trabalho são giradas para cima ou para baixo, elas são atribuídas à política correta automaticamente. Isso economiza recursos consideráveis, eliminando a necessidade de movimentos manuais, adições ou alterações.

Independente de infraestrutura: uma das principais vantagens da segmentação definida por software é que ela é independente da infraestrutura. A mesma ferramenta oferece visibilidade e segmentação em qualquer infraestrutura: bare metal, virtualizada, PaaS, nuvem, contêineres, etc. Tudo sob um painel de controle e com um fluxo de trabalho único. Isso resulta em uma liberdade operacional significativa na qual os padrões de segurança podem ser alcançados sem qualquer restrição à escolha da infraestrutura subjacente.

Mais receita, relacionamentos mais sólidos: o mais importante é que isso introduz uma oportunidade significativa para os operadores de data center. Embora eles gerenciem e forneçam a segmentação interna, eles podem aproveitar o treinamento, as ferramentas e os processos para oferecer um serviço gerenciado muito necessário para seus clientes, administrando a segmentação não apenas para os aplicativos hospedados, mas também para aplicativos que estão nas instalações do cliente ou na nuvem dentro da mesma ferramenta, dentro do mesmo painel de controle. Isso não só resulta em potencial de receita adicional, mas também cria uma dependência mais forte do operador, resultando em relacionamentos mais longos e lucros mais altos.

Por que a Akamai

Para oferecer esses benefícios, uma solução de segmentação definida por software deve atender a vários critérios essenciais. Ela deve permitir uma visibilidade profunda no nível do processo de todos os aplicativos em execução no ambiente de computação e a capacidade de mapear todos os fluxos de dados entre eles. A flexibilidade para rotular adequadamente os ativos para a criação de políticas e modificar automaticamente os rótulos à medida que as cargas de trabalho se dimensionam automaticamente são também essenciais para a implantação e o gerenciamento eficientes. E a solução precisa ser independente de plataforma e infraestrutura. As políticas devem ser capazes de seguir seus respectivos aplicativos e ter um desempenho consistente entre vários ambientes. Por fim, a solução deve permitir um modelo operacional automatizado e simplificado para a criação, o gerenciamento e a aplicação de políticas.

Somente a Akamai Guardicore Segmentation atende a todos esses critérios. A segmentação definida por software é nossa principal capacidade. A solução oferece uma visualização gráfica sem precedentes de todos os ativos no ambiente e das dependências entre eles, sejam bare metal, máquinas virtuais, nuvem pública, contêineres ou dispositivos de IoT. Essa visibilidade profunda acelera drasticamente o processo de identificação, agrupamento e criação de políticas de segurança em torno de microssegmentos de aplicativos.

Para obter mais informações, visite akamai.com/guardicore.