Akamai

Desvendando os sete mitos sobre microssegmentação

Pode parecer contraintuitivo pensar pequeno ao dimensionar grande, mas há muitos equívocos em torno de soluções modernas de microssegmentação.

Você acha que encontrará tempo de inatividade da rede ou dificuldades para operacionalizar uma implantação definida por software? Pense novamente. Eis o que é importante quando se trata de se tornar granular.

Mito 1

Minha solução EDR é suficiente para impedir ataques de ransomware

A detecção e resposta do ponto de extremidade (EDR) e a segmentação abordam ataques de ransomware, mas em diferentes estágios da cadeia de destruição e de diferentes maneiras. As soluções de EDR visam detectar a presença de ransomware em execução ou executando em dispositivos ou pontos de extremidade que estão monitorando. Se o EDR detectar ransomware, ele pode encerrar o processo, colocar o dispositivo em quarentena e, às vezes, reverter qualquer criptografia que tenha ocorrido. EDR e segmentação são complementares: caso o EDR não detecte ransomware, as soluções de segmentação compartimentam a rede em compartimentos fechados para limitar o movimento lateral (leste-oeste) de um ataque. Com ransomware, deve ocorrer movimento lateral para que os invasores sejam bem-sucedidos. A segmentação garantirá que os ataques que conseguiram avançar além do ponto de extremidade acabem por atingir uma barreira, limitando a zona de explosão de uma infecção inicial. Leia mais sobre as diferenças entre EDR e segmentação.

1h42m

é o tempo médio para um agente de ameaças começar a se mover lateralmente dentro da rede, uma vez que tenha uma posição inicial

(Relatório de defesa digital da Microsoft 2022)

Mito 2

Já estou fazendo segmentação

A segmentação não é um conceito novo, mas está cada vez mais sofisticada. Há décadas, as organizações têm usado um patchwork de VLANs, firewalls internos, ACLs e grupos de segurança para segmentar seus ambientes. Mas esses métodos legados não evoluíram para atender às demandas complexas da infraestrutura moderna híbrida e multinuvem, criando lacunas defensivas e pontos cegos por meio da subsegmentação.

Por exemplo: Os firewalls herdados não mapeiam ou avaliam as dependências do fluxo de trabalho, dificultando a identificação de segmentações para aplicações, cargas de trabalho ou usuários. Portanto, as empresas são forçadas a implementar amplas políticas de segmentação que são excessivamente permissivas e podem, de forma fácil *e rápida*, resultar em configurações incorretas perigosas que são difíceis e complicadas de solucionar problemas.

Com a microssegmentação, as organizações podem segmentar e aplicar até a Camada 7, muito além do possível com as ferramentas de segmentação tradicionais.

Redução de custo de

US$ 2 milhões

na atualização de firewalls em três anos

(TEI da Forrester)

Mito 3

A microssegmentação é muito difícil de operacionalizar

A microssegmentação moderna está pronta para implantação empresarial, agora mais do que nunca.

Com o Akamai Guardicore Segmentation, as eficiências operacionais máximas são obtidas por meio do uso de uma única solução baseada em software para segmentação, visibilidade, criação de políticas e aplicação em todos os ambientes, desde o data center e a nuvem até ativos baseados em contêiner. Após a implantação, o Akamai Guardicore Segmentation cria um mapa visual dinâmico de toda a infraestrutura de TI que permite que as equipes de segurança visualizem a atividade até o nível de processo individual, em tempo real e histórico.

Essas percepções detalhadas sobre o comportamento das aplicações podem ser usadas para criar políticas granulares de microssegmentação rapidamente por meio de uma interface visual intuitiva. Regras de negação global, zoneamento de aplicações críticas e a capacidade de segmentar imediatamente ambientes grandes significam tempo rápido de retorno e risco reduzido.

Com os métodos de segmentação herdados, você não tem visibilidade para saber por onde começar.

Aumento de

↑95%

na produtividade do SecOps

(TEI da Forrester)

Mito 4

Microssegmentação significa tempo de inatividade de aplicações e de rede

Com as abordagens tradicionais de segmentação, as aplicações geralmente são movidas entre sub-redes ou VLANs, causando tempo de inatividade e interrompendo a continuidade dos negócios. Os engenheiros de rede e os administradores de firewall ainda precisam planejar o tempo de inatividade programado, alterar o controle ou as janelas de manutenção, aumentando o tempo de implantação de novos serviços ou atualizações de aplicações. Pior ainda, esses atrasos podem resultar em maior risco devido à exposição de ativos e à vulnerabilidade.

A segmentação definida por software, por outro lado, separa a segurança da infraestrutura subjacente e dos sistemas operacionais para que a segmentação possa ser realizada de forma independente, sem tocar na rede ou na aplicação. Se houver um evento, em vez de isolar completamente as máquinas afetadas, somente o vetor de ataque será bloqueado, limitando o impacto negativo para a empresa.

A microssegmentação também pode ser implantada no modo de alerta para permitir o teste de políticas em ambientes de produção ao vivo sem o risco do tempo de inatividade. A conclusão: As soluções de segmentação modernas não devem ser uma escolha entre melhor segurança e agilidade nos negócios.

Mito 5

A microssegmentação não cobre meu ambiente de IoT ou tecnologia operacional

Você sabia que as políticas Zero Trust podem ser impostas para dispositivos de Internet das coisas e tecnologia operacional que não conseguem executar software de segurança baseado em host?

Nossos recursos de segmentação sem agente preenchem a lacuna defensiva entre dispositivos que não podem executar agentes para eliminar pontos cegos de visibilidade, como pontos de extremidade sem espaço.

Essa cobertura estendida é especialmente importante para ambientes de saúde, varejo e fabricação com muitos dispositivos IoT conectados à rede (e vulneráveis) e sistemas de tecnologia operacional herdados. A integração da segmentação sem agente à sua infraestrutura de rede permite a descoberta automática de novos dispositivos, impressões digitais e aplicação de políticas para ajudar a reduzir os riscos e, ao mesmo tempo, acelerar a jornada da empresa para o Zero Trust.

Mito 6

Um agente de microssegmentação adiciona muita latência

Um dos maiores equívocos em relação à microssegmentação é a latência adicional.

Na realidade, o uso de políticas de segmentação distribuídas baseadas em software, em vez de forçar todo o tráfego através de pontos de estrangulamento de firewall específicos, elimina os gargalos da rede. Por padrão, o agente Akamai Guardicore é altamente otimizado para trabalhar com sistemas operacionais Linux, Unix, Windows e Mac e não consome recursos substanciais.

E como o agente não está em linha, ele não realiza inspeção profunda de pacotes que pode adicionar à latência.

Em vez disso, o agente Akamai Guardicore obtém o mínimo de informações do cabeçalho do pacote para formar uma visão completa do ambiente do cliente. Se você está procurando velocidade *e* desempenho, sim, *você pode* ter tudo.

Mito 7

A microssegmentação significa contratar FTEs impossíveis de encontrar

Com os CISOs sentindo a pressão para "fazer mais com menos", as soluções de segurança devem tirar o peso das costas dos defensores, não consumindo mais recursos internos escassos.

Métodos tradicionais de segmentação, como o gerenciamento de firewalls e VLANs, envolvem processos dolorosos e de várias etapas, envolvendo muitas equipes, separadamente responsáveis por comutação, roteamento, implementação de firewall e criação de políticas de segurança. Uma implementação de firewall legado pode levar de 14 a 22 semanas em média. Tudo isso contribui para os cronogramas do projeto, sujeitando a organização a custos de mão de obra significativos e sobrecargas operacionais.

Em contraste, a solução definida por software da Akamai leva em média duas semanas para ser implantada e apenas um funcionário em tempo integral. E, ao adicionar o Akamai Hunt, nosso serviço gerenciado de busca de ameaças, você economizará tempo e recursos monitorando seu ambiente quanto a ataques emergentes, movimentos laterais e comportamento de ataque atípico.

Atualmente, o talento cibernético é difícil de contratar e ainda mais difícil de reter. É hora de as defesas funcionarem a favor, *e não contra*, da sua organização.

Principais estatísticas

106%

ROI comprovado de até aproximadamente 106% em 12 meses

(TEI da Forrester)

Como a Akamai pode ajudar

O Akamai Guardicore Segmentation é uma solução de microssegmentação baseada em software que oferece a maneira mais simples, rápida e intuitiva de impor os princípios Zero Trust. Ele permite a prevenção de movimentos laterais mal-intencionados em sua rede por meio de políticas precisas de segmentação, visão da atividade no ambiente de TI e alertas de segurança de rede. O Akamai Guardicore Segmentation opera em data centers, ambientes multinuvem e pontos de extremidade. Sua implantação é mais rápida do que abordagens de segmentação de infraestrutura e oferece visibilidade e controle inigualáveis de sua rede.

Saiba como o Akamai Guardicore Segmentation permite proteção granular, visibilidade profunda e aplicação consistente de políticas de segurança em escala para manter seus dados mais confidenciais protegidos.