WHITE PAPER

Explorando os principais casos de uso de microssegmentação

Por John Grady, analista sênior do Enterprise Strategy Group

Janeiro de 2023

Este white paper do Enterprise Strategy Group foi encomendado pela Akamai e distribuído sob licença da TechTarget, Inc.

Conteúdo

Sumário executivo

O zero trust se difundiu por todo o setor de segurança cibernética. No entanto, a amplitude da iniciativa e os pontos de vista conflitantes sobre o que é mais importante para a estratégia geraram confusão, no que diz respeito a onde começar e quais ferramentas suportam melhor a estrutura. Embora não haja um único caminho para o zero trust, a estratégia depende, em última análise, de garantir que os recursos e as entidades só possam se comunicar uns com os outros quando expressamente permitido pela política, indicando a importância da microssegmentação.

Atualmente, o uso de ferramentas de microssegmentação é um pouco limitado, mas espera-se que ele aumente de forma significativa em reconhecimento à importância da microssegmentação para o zero trust e à sua aplicabilidade a uma grande variedade de casos de uso. Quer as organizações estejam considerando o zero trust para evitar ameaças, promover a eficiência em toda a empresa ou modernizar sua abordagem de segurança geral, a microssegmentação poderá ajudar. Em especial, a abordagem de microssegmentação baseada em software e com suporte de inteligência artificial da Akamai oferece visibilidade granular e permite que as organizações evitem movimentos laterais, interrompam ataques de ransomware e apliquem princípios de zero trust de forma consistente em todo o ambiente.

Quer as organizações estejam considerando o zero trust para evitar ameaças, promover a eficiência em toda a empresa ou modernizar sua abordagem de segurança geral, a microssegmentação poderá ajudar.

O zero trust está avançando, mas é fundamental estabelecer prioridades claras

Os ambientes empresariais continuam crescendo em complexidade à medida que os recursos passam para a nuvem; os modelos de negócios digitais se consolidam e os usuários se tornam cada vez mais distribuídos. Essas mudanças dificultam inerentemente o trabalho da equipe de segurança cibernética, pois os invasores procuram passar por brechas nas defesas para lançar ataques de ransomware, roubar informações dos clientes ou extrair propriedade intelectual confidencial. Infelizmente, as abordagens de segurança tradicionais que se baseiam em controles altamente permissivos baseados em perímetro não podem mais lidar com essas realidades, o que força as equipes de segurança a reavaliarem as estratégias. Além disso, os ataques estão crescendo em número e sofisticação, o que impossibilita que as equipes de segurança se mantenham atualizadas, solucionem e façam patches contra todas as ameaças em potencial.

Esses problemas levaram muitas delas ao conceito de zero trust. Embora não sejam novas, as estratégias de zero trust têm despertado um interesse significativo nas organizações como um caminho para uma abordagem mais dinâmica, menos privilegiada e baseada em risco para a segurança cibernética. Uma abordagem zero trust elimina a confiança implícita do ambiente e valida continuamente cada interação digital. Como resultado, uma abordagem zero trust deve dar às equipes de segurança maior confiança de que seus recursos, usuários e dispositivos permanecerão seguros e disponíveis. No entanto, a extensa aplicabilidade do zero trust, juntamente com pontos de vista e definições por vezes conflitantes sobre o que é esse modelo, criou confusão e pode dificultar a identificação de um ponto de partida pelas organizações.

Avaliar as prioridades organizacionais e os resultados desejados pode ajudar a restringir o foco e determinar onde começar com uma iniciativa de zero trust. Há diversos impulsionadores de negócios que estimulam as organizações a atingir o zero trust (veja a Figura 1).[1] O objetivo mais comum é a modernização da segurança cibernética, citada por 51% dos entrevistados. Essa mentalidade foi enfatizada pelo

O zero trust depende de garantir que os recursos e as entidades só possam se comunicar entre si quando expressamente permitido pela política.

[1] Fonte: resultados da pesquisa do Enterprise Strategy Group, *The State of Zero Trust Security Strategies,* maio de 2021.

governo federal dos EUA por meio de ordens executivas sobre segurança cibernética emitidas pela administração de Biden, que colocou a arquitetura zero trust em seus requisitos de modernização. Embora não seja direcionada diretamente ao setor privado, essas ordens podem ajudar a fornecer orientação para equipes de segurança fora do governo federal. Outras metas estratégicas para o zero trust incluem o suporte à transformação digital (35%) e a aceleração da adoção da nuvem (34%). Esses fatores destacam as expectativas que muitas organizações têm de que a equipe de segurança deve ajudar a capacitar a empresa, em vez de simplesmente proteger os ativos. Objetivos mais estratégicos, como reduzir o número de incidentes de segurança (43%), permitir acesso remoto seguro (41%), simplificar a conformidade (31%) e impedir a extração de dados (30%) também são comuns.

Figura 1. Impulsionadores para o Zero Trust

Fonte: Enterprise Strategy Group, uma divisão da TechTarget, Inc.

Em alguns casos, limitar o foco inicial de um projeto zero trust pode certamente ajudar a equipe de segurança a identificar as ferramentas necessárias para apoiar a estratégia. Por exemplo, se o objetivo for melhorar o acesso remoto seguro para funcionários e terceiros, muitas equipes irão optar pelo acesso à rede zero trust (ZTNA). Ferramentas de identidade, como a autenticação multifator (MFA), também podem entrar em ação nesse cenário. No entanto, alguns impulsionadores podem deixar os requisitos de tecnologia abertos à interpretação e, muitas organizações, mesmo depois de fazer alguma redução, acabam se concentrando em objetivos diversos. Nessas situações, é importante que as organizações identifiquem ferramentas e práticas que possam dar suporte a uma grande variedade de casos de uso e resultados.

A microssegmentação está atualmente subutilizada no suporte a um modelo zero trust

Embora não haja um caminho único para o zero trust, a estratégia depende, em última análise, de garantir que os recursos e as entidades só possam se comunicar uns com os outros quando expressamente permitido pela política. Isso significa que um elemento-chave para a filosofia zero trust de qualquer organização deve ser a capacidade de garantir a segmentação adequada dos ativos para ajudar a limitar os impactos de ataques bem-sucedidos. Isso pode ser aplicável a uma meta ampla, como modernização da segurança cibernética, ou a um objetivo mais específico, como a prevenção contra a extração de dados.

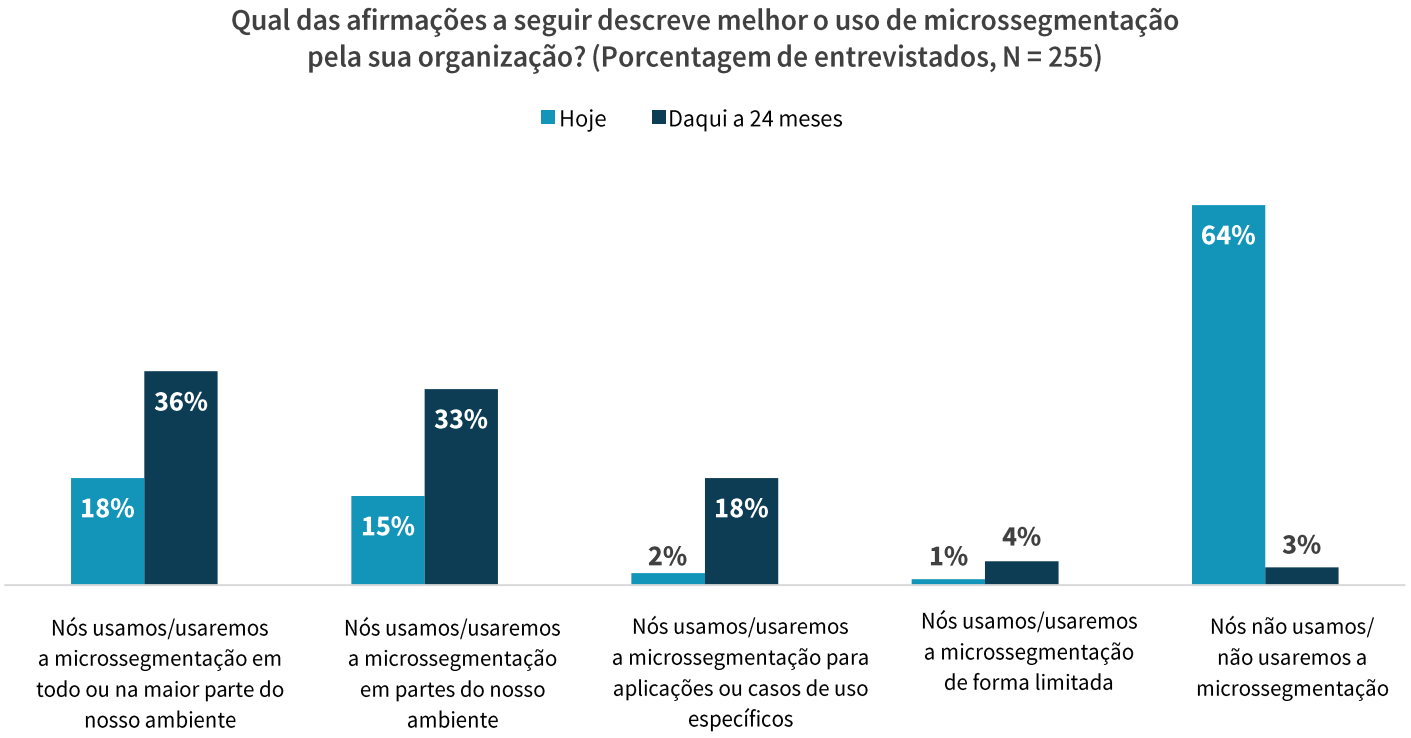
No entanto, no ambiente atual, a segmentação com granulação grossa geralmente não é suficiente, e uma microssegmentação mais granular é necessária para proteger adequadamente os ativos corporativos. As arquiteturas de aplicações modernas geralmente dependem de cargas de trabalho distribuídas em várias instâncias de servidor e, em alguns casos, em vários ambientes de nuvem. A prática de segmentação de recursos com base no local ficou ultrapassada e não aborda os desafios que as equipes de segurança enfrentam atualmente.

Historicamente, as organizações têm hesitado em adotar ferramentas de microssegmentação. A pesquisa feita pelo Enterprise Strategy Group (ESG) da TechTarget descobriu que 28% das organizações acreditam que a microssegmentação é muito complexa. No entanto, isso provavelmente se deve, em grande parte, ao fato de que as equipes de segurança usam ferramentas inadequadas para a microssegmentação. Especificamente, a pesquisa do ESG descobriu que 55% das organizações relatam o uso de ferramentas baseadas em infraestrutura para microssegmentação, como firewalls, enquanto apenas 8% usam ferramentas baseadas em host.[2] Os firewalls não conseguem aplicar as políticas granulares necessárias para que a microssegmentação seja bem-sucedida. Além disso, essas ferramentas fornecem visibilidade limitada em todas as cargas de trabalho de aplicações e têm dificuldade para lidar de forma consistente com todos os aspectos do ambiente, tanto no local quanto na nuvem.

Isso fez com que a microssegmentação fosse subutilizada. Apesar de sua importância para o zero trust, apenas 36% das organizações usam a microssegmentação atualmente, de acordo com a pesquisa do ESG (veja a Figura 2). A boa notícia é que muitas organizações reconhecem que essa é uma lacuna significativa em suas defesas. Como resultado, 91% preveem usar a microssegmentação nos próximos 24 meses.[3] Em última análise, a microssegmentação consolida e reforça os principais benefícios do zero trust, reforçando as redes físicas, virtuais e de nuvem contra ameaças externas e internas. Ela deve ser um componente essencial de qualquer estratégia de zero trust.

[2] Fonte: resultado da pesquisa completa do Enterprise Strategy Group, *Network Security Trends in Hybrid Cloud Environments,* dezembro de 2021.
[3] Ibid.

Figura 2. Adoção da microssegmentação



Fonte: Enterprise Strategy Group, uma divisão da TechTarget, Inc.

Principais casos de uso de microssegmentação

A microssegmentação pode ser aplicada de forma ampla a diversos casos de uso de zero trust, o que é um motivo significativo pelo qual ela está ganhando mais destaque do que nunca. No entanto, antes de mais nada, a microssegmentação fornece um bom ponto de partida para uma jornada zero trust, pois pode proteger os ativos mais críticos de uma organização, especialmente se a solução utilizada fornecer visibilidade altamente granular em relacionamentos de carga de trabalho e entidade. Desenvolver uma linha de base de fluxos de tráfego e dependências é fundamental para qualquer esforço de zero trust como um primeiro passo para remover a confiança implícita sem perturbar os negócios. Essa abordagem permite que as equipes de segurança protejam rapidamente seus ativos mais críticos para ajudar a limitar os impactos em caso de violação enquanto uma implementação zero trust está sendo realizada. Com essa garantia em vigor, as equipes de segurança podem voltar sua atenção para alguns dos outros casos de uso suportados pela microssegmentação.

Prevenção de ameaças

Zero trust é uma estrutura de segurança, e o objetivo da segurança é proteger a organização contra ameaças virtuais. Portanto, podemos concluir que alguns dos principais casos de uso de microssegmentação se concentram na prevenção de ameaças e na limitação de seus impactos nos recursos corporativos, especificamente:

- Delimitação de ativos críticos. As equipes de segurança devem ponderar e equilibrar os riscos ao decidir onde priorizar as proteções. Aplicações de alto valor que contêm informações regulamentadas de clientes, propriedade intelectual ou outras informações confidenciais devem receber mais atenção e controles de segurança aprimorados devido ao impacto potencial do comprometimento desses sistemas. Com a microssegmentação, as equipes de segurança podem assegurar que essas aplicações e as cargas de trabalho que as compõem sejam totalmente separadas do restante da infraestrutura.
- Limitação do movimento lateral. Um princípio subestimado do zero trust é trabalhar sob uma mentalidade de "pressupor violação", presumindo que os adversários têm acesso à rede corporativa. A proliferação de pontos de extremidade tradicionais, servidores, recursos de nuvem e até mesmo dispositivos inteligentes torna as invasões inevitáveis. Como resultado, limitar o raio de destruição de um ataque potencial por meio da microssegmentação pode impedir que os invasores tenham a capacidade de se mover lateralmente pela rede.

Proteção contra ransomware

A prevalência contínua de ransomware e o impacto desses ataques elevaram o problema para um nível executivo, ou até mesmo de diretoria. Embora a prevenção para ransomware exija não apenas uma segurança forte, mas também uma boa proteção de dados e recursos de resposta a incidentes, a microssegmentação pode ajudar as organizações a garantir que elas tenham uma base sólida para combater um ataque. Os invasores geralmente visam informações confidenciais e sistemas durante um ataque, somente depois de penetrar no ambiente e dedicar um tempo para fazer o reconhecimento. Quando a microssegmentação é usada para delimitar ativos críticos e limitar o movimento lateral, os invasores têm menos liberdade de se mover pelo ambiente. Além disso, quando um ataque de ransomware é descoberto, uma organização que usa microssegmentação pode rapidamente fechar as vias de comunicação que os invasores usam e isolar servidores infectados para evitar que o ataque se propague ainda mais.

- Detecção e resposta de ameaça. No caso de um ataque, o tempo é essencial. As ferramentas de microssegmentação podem ajudar as equipes de segurança a responder de forma rápida e eficaz, identificando rapidamente possíveis caminhos de ataque com base nas relações com aplicações, bloqueando as portas que os invasores usam durante um ataque e isolando rapidamente os sistemas afetados do resto da rede. Elas também limitam o ataque ao seu ponto inicial de entrada.

Promover a eficiência em toda a empresa

Embora o primeiro objetivo da equipe de segurança seja proteger o ambiente, o estatuto atual também exige que isso seja feito sem afetar a eficiência da empresa. Além disso, se as equipes de segurança puderem realmente ajudar a capacitar seus colegas, os negócios irão melhorar por conta disso. Isso pode assumir uma variedade de significados, mas alguns dos mais comuns incluem:

- Suporte à adoção da nuvem. A mudança para a nuvem não é novidade, mas as preocupações com a segurança continuam sendo a prioridade número um de muitas organizações. Algumas delas se devem à falta de familiaridade com os controles de segurança nativos em plataformas de infraestrutura como serviço, e algumas se devem

à inconsistência de segurança que pode surgir em ambientes de nuvem híbrida. A microssegmentação proporciona às organizações maior confiança, pois os controles podem ser usados em todos os aspectos do ambiente e fornecem uma melhor consistência de segurança em cenários de nuvem híbrida.

- Possibilitar a modernização de aplicações. Além da mudança para a nuvem, a adoção de arquiteturas de aplicações modernas, como contêineres, continua a aumentar. Esses modelos permitem que as equipes de aplicações projetem, criem e implantem aplicações mais rápido do que nunca. As ferramentas que podem garantir que esses recursos estejam protegidos, e isso sem limitar a velocidade dos desenvolvedores, criam um impacto positivo nos negócios. As ferramentas de microssegmentação, que fornecem visibilidade dos fluxos de tráfego em ambientes de contêiner e aplicam automaticamente políticas de segmentação conforme os contêineres são disponibilizados online ou movidos, podem ajudar as equipes de desenvolvimento a garantir que suas aplicações estejam seguras.

- Simplificação da conformidade. As questões regulatórias consomem uma quantidade cada vez maior de tempo, orçamento e atenção de uma organização. Garantir que os riscos de segurança sejam isolados o máximo possível para limitar o potencial de problemas, como violações de privacidade de dados ou perda de informações pessoalmente identificáveis, pode tornar o processo muito menos oneroso. A microssegmentação pode garantir que os sistemas sujeitos a exigências de conformidade sejam isolados do resto do ambiente, o que pode reduzir a pressão sobre as equipes de segurança.

Segmentação zero trust

Um dos aspectos mais atrativos da microssegmentação é que ela pode fornecer um valor imediato às organizações quando voltada a casos de uso muito específicos. A capacidade de começar com a lista de bloqueio, as aplicações críticas de delimitação, a segmentação do ambiente e outras políticas menos complicadas que fornecem um valor rápido com relativa facilidade pode ser atrativa para muitas organizações. Poucas organizações, se é que alguma, implantam uma estratégia de microssegmentação completa em toda a empresa de uma só vez. Mas, à medida que a microssegmentação for implantada de forma mais ampla em todo o ambiente no âmbito de uma iniciativa zero trust, muitas organizações começarão a abordar a segmentação zero trust. Ela combina os casos de uso e os resultados positivos discutidos anteriormente, pois as organizações são capazes de manter uma visibilidade abrangente e granular sobre os fluxos de tráfego, proteger seus ativos mais confidenciais, impedir a movimentação lateral e responder rapidamente às ameaças, tudo isso ao mesmo tempo em que capacita melhor os negócios. Embora não seja o ponto de partida para muitos projetos de microssegmentação, isso deve ser visto como um objetivo a ser almejado ao longo do tempo.

Abordagem da Akamai para microssegmentação

A solução Akamai Guardicore Segmentation é uma abordagem baseada em software para a microssegmentação, projetada para impedir que os agentes de ameaça alcancem movimentos laterais em todo o ambiente digital.

É importante que as organizações tenham em mente que, embora a microssegmentação seja um aspecto importante do zero trust, também existem outros componentes-chave, exigindo outras tecnologias que suportem detecção e resposta de ameaças, identidade, segurança de dados e muito mais. Avaliar, selecionar e trabalhar com fornecedores de tecnologia é um processo metódico e orientado a detalhes que pode fazer a diferença entre atender às metas de segurança cibernética da organização e algo que consuma dinheiro, tempo e recursos da força de trabalho. Como resultado, considerar o uso das ferramentas de microssegmentação, que oferecem um amplo conjunto

de integrações e recursos de compartilhamento de sinal, pode ajudar a promover uma estratégia zero trust para além da microssegmentação, bem como a reduzir a complexidade operacional.

A Akamai, uma empresa consagrada de infraestrutura de rede, fez da microssegmentação e do zero trust as partes centrais de seu portfólio de soluções. O conhecimento da empresa sobre os requisitos de infraestrutura corporativa para ambientes locais e em nuvem incluiu a experiência na identificação e no trabalho através de possíveis desafios de segurança cibernética.

A Akamai Guardicore Segmentation é uma abordagem baseada em software para microssegmentação projetada para impedir que os agentes de ameaça alcancem movimentos laterais em todo o ambiente digital. Ela usa visibilidade granular para impor princípios de zero trust no nível da rede, ajudando as organizações a visualizar a atividade e a movimentação dentro do ambiente físico e virtual. Sua estrutura de segmentação baseada em inteligência artificial usa modelos integrados para identificar e impedir incursões, como ransomware, ataques baseados em endpoint e ataques remotos orientados à força de trabalho. Ela pode ser usada em diversas plataformas, incluindo servidores bare-metal, máquinas virtuais, contêineres, dispositivos de IoT e instâncias de nuvem.

A Akamai Guardicore Segmentation coleta dados abrangentes sobre a infraestrutura subjacente de várias maneiras, como sensores baseados em agentes, coleta de dados baseada em rede, registros de fluxo de nuvem privada virtual e integrações que promovem a funcionalidade sem agente. O mapeamento dinâmico oferece aos administradores uma visão completa das atividades com granularidade grossa. Devido à experiência da Akamai em ambientes de rede corporativa, a Akamai Guardicore Segmentation foi projetada para escalabilidade empresarial e desempenho consistente, identificando e evitando fontes de gargalos de tráfego.

A grande verdade

A microssegmentação não é uma tecnologia nova. Na verdade, ela pode ter estado à frente do seu tempo. Mas nunca é demais enfatizar a importância da microssegmentação na proteção de ambientes modernos de múltiplas nuvens e híbridos e, especificamente, na operacionalização de estratégias de zero trust. A microssegmentação oferece a flexibilidade, a agilidade e a eficiência necessárias para habilitar o zero trust em vários casos de uso essenciais e críticos para os negócios, protegendo tudo, desde a infraestrutura crítica e a propriedade intelectual até identidades e credenciais. A experiência da Akamai em infraestrutura de rede, segmentação e microssegmentação a torna um candidato viável para ajudar a planejar, criar, implantar e até mesmo gerenciar a infraestrutura segura baseada em ferramentas e mentalidades de microssegmentação.

Enterprise Strategy Group by TechTarget

Enterprise Strategy Group é uma empresa integrada de análise de tecnologia, pesquisa e estratégia que fornece inteligência de mercado, insights práticos e serviços de conteúdo go-to-market para a comunidade global de TI.

www.esg-global.com contact@esg-global.com 508.482.0188