Akamai

WHITE PAPER

O estado da segmentação em 2023

A superação dos obstáculos de implementação prova ser transformadora

Índice

Introdução

Nunca foi fácil para os departamentos de segurança de TI. Mas agora, invasores cada vez mais sofisticados estão combinando técnicas para criar ameaças maiores e mais frequentes, colocando as equipes de segurança sob uma pressão maior do que nunca. Nenhuma empresa pode operar sem uma presença online, e uma violação bem-sucedida pode causar danos extensos, se não irreparáveis, à reputação e à receita.

Como mostram as conclusões deste relatório, esses ataques também estão tendo um impacto maior, aumentando a pressão sobre os líderes de segurança para que escolham as soluções certas e mantenham todo o ambiente seguro, sem sacrificar o desempenho geral ou a inovação.

Ao atualizar as conclusões deste relatório desde 2021, queríamos descobrir se a segmentação era a solução escolhida e se era eficaz. Os 1.200 participantes concordaram de forma esmagadora com a eficácia da segmentação para manter os ativos protegidos, mas o progresso geral na implementação dessa segmentação em aplicativos e ativos comerciais essenciais foi menor do que o esperado. Em todas as regiões, o principal obstáculo foi a falta de conhecimento para implementar a segmentação, o que sugere que as equipes podem estar hesitantes em embarcar em um projeto que poderia prejudicar o desempenho, especialmente devido à crescente complexidade dos ambientes de TI.

A boa notícia? A perseverança compensa. A segmentação provou ter um efeito transformador na defesa para aqueles que segmentaram a maioria de seus ativos essenciais, permitindo que eles mitigassem e contivessem o ransomware 11 horas mais rápido do que aqueles com apenas um ativo segmentado. Imagine a diferença que essas 11 horas fazem para sua equipe, clientes, reputação da marca e receita.

Os ataques de ransomware continuam aumentando, assim como seu impacto

O número de ataques de ransomware (bem-sucedidos e malsucedidos) dobrou nos últimos dois anos, de 43 em média em 2021 para 86 em 2023. Um aumento ainda maior foi medido entre o primeiro trimestre de 2022 e o primeiro trimestre de 2023 pelos dados coletados dos sites de vazamento de aproximadamente 90 grupos diferentes de ransomware. Lançado em agosto de 2023, o relatório Ransomware à espreita: o avanço de técnicas de exploração e a busca ativa por dias zero cita que o uso de vulnerabilidades de dia zero e de dia um levou a um aumento de 143% no total de vítimas de ransomware em todo o mundo.

Não é de surpreender que as empresas dos EUA ainda enfrentem o maior número de ameaças de ransomware (Figura 1): as equipes de segurança de TI e os tomadores de decisão desse país relataram uma média de 115 ataques de ransomware nos últimos 12 meses, o maior número entre todos os países avaliados.

Número médio de ataques de ransomware nos últimos 12 meses, por país

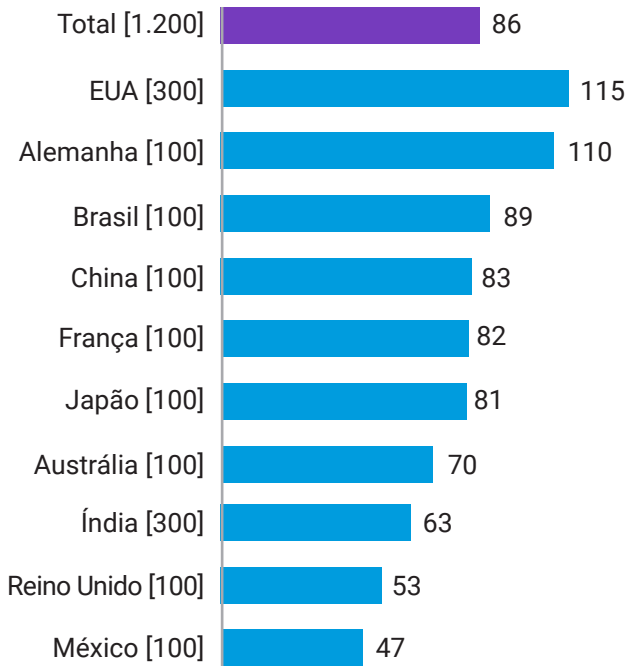

Fig.1: quantos ataques de ransomware foram feitos contra sua organização nos últimos 12 meses (independentemente de terem sido bem-sucedidos ou não)? [1.200], mostrando apenas o número médio de ataques nos últimos 12 meses, divididos por país.

Considerando que os EUA estão entre os dois países com menor probabilidade de ter implementado a segmentação em mais de duas áreas de negócios de missão crítica (Figura 2), sua posição no topo em ataques de ransomware e sua baixa classificação na implementação da segmentação podem estar relacionadas.

Obviamente, o alto número de ataques de ransomware nos EUA provavelmente pode ser atribuído a uma série de fatores, incluindo a atenção midiática recebida após grandes violações, como a que um grupo russo de crimes cibernéticos cometeu contra agências federais em 2023 e a proliferação de dispositivos de Internet das coisas nos EUA (dois bilhões a mais do que a China, que ocupa o segundo lugar). O ransomware para IoT (R4IoT) explora dispositivos de IoT vulneráveis, como câmeras IP, para obter uma base inicial e, em seguida, move-se lateralmente em uma rede de TI, aproveitando-se de práticas de segurança inadequadas para manter reféns os processos de missão crítica.

Os ataques de ransomware não são apenas mais frequentes globalmente em 2023 em comparação com 2021, mas seus impactos são mais bem-sucedidos (Figura 3), com nossos entrevistados indicando aumentos no tempo de inatividade da rede, na perda de dados e nos danos à reputação — o que aumenta significativamente os riscos para as equipes de segurança. Vemos o efeito dessa pressão também em termos de estratégia: o número de organizações que estão atualizando continuamente as estratégias ou políticas de cibersegurança aumentou de 5% em 2021 para 13% em 2023, não apenas em resposta ao ransomware, mas também a uma superfície de ataque em constante mudança. Forças de trabalho distribuídas e aplicativos e dados migrando para a nuvem são apenas dois fatores que afetam a estratégia de segurança diariamente.

Aqueles que segmentaram mais de dois ativos/áreas por país

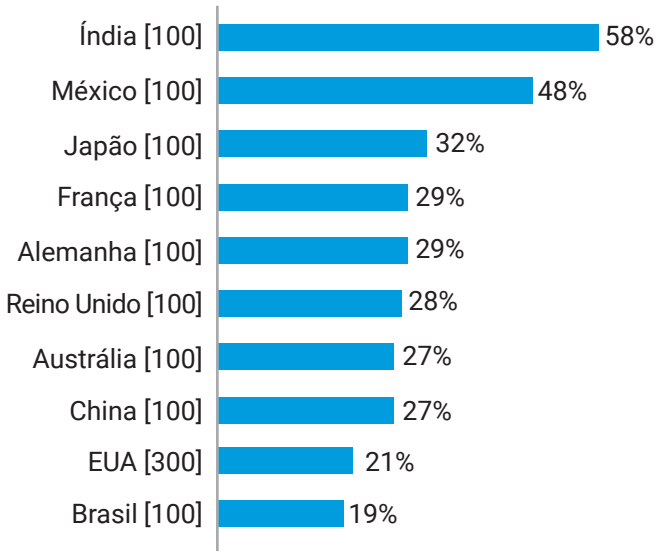

Fig. 2: para cada uma das seguintes medidas de segurança de TI, quais ativos, se houver, estão sendo cobertos? [1.200], mostrando as respostas apenas para a medida de segurança de segmentação e as porcentagens que estão usando a segmentação para proteger os principais ativos, divididas por país.

Impacto de ataques cibernéticos e de ransomware

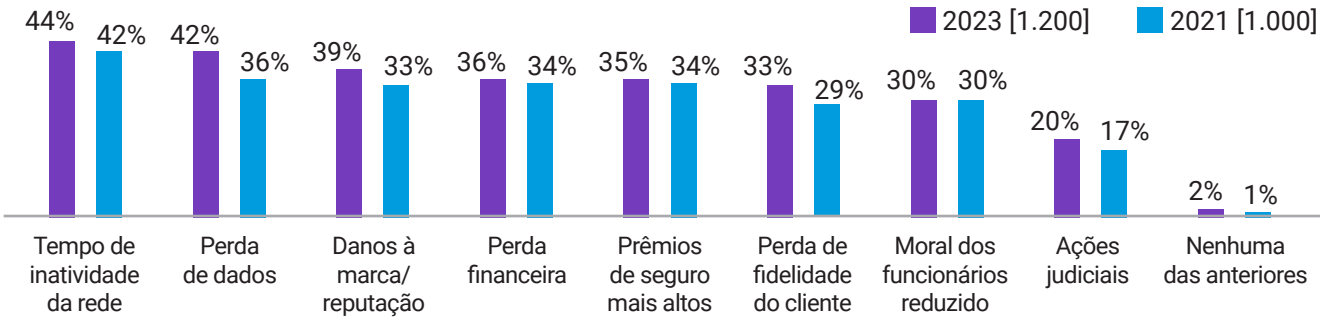

Fig. 3: quando sua organização detectou anteriormente ransomware ou algum outro ataque cibernético, qual dos seguintes impactos teve em sua organização? [Tamanhos da base no gráfico], não mostra todas as opções de resposta, divididas por dados históricos.

Conclusões regionais

É mais provável que os ataques cibernéticos atinjam as pessoas nas Américas: o número total de ataques de ransomware é maior nas Américas, com 96 ataques em média nos últimos 12 meses, em comparação com 83 na EMEA e 75 na APAC.

A segmentação e a microssegmentação são consideradas mais importantes na APAC e nas Américas do que na EMEA: as equipes de segurança de TI e os tomadores de decisão na APAC (62%) e nas Américas (60%) têm maior probabilidade de dizer que a segmentação da rede é extremamente importante para garantir a segurança da organização do que os da EMEA (53%).

As pessoas nas Américas têm maior probabilidade de dizer que a microssegmentação é a principal prioridade (41%) do que as contrapartes na APAC (35%) ou na EMEA (23%).

É mais provável que as empresas da EMEA não tenham feito nenhuma segmentação: é muito mais provável que as organizações digam que nenhum ativo crítico para os negócios foi segmentado na EMEA (10%) do que na APAC (4%) ou nas Américas (1%).

As taxas mais lentas de implementação, ou seja, aquelas sem áreas segmentadas, foram observadas no Reino Unido (23%), com equipamentos antigos relatados como o principal obstáculo (46%).

As organizações da APAC foram as que mais se segmentaram: é mais provável que as organizações da APAC tenham segmentado mais de dois ativos essenciais aos negócios (36%) do que as da EMEA (29%) ou das Américas (26%).

As organizações, em todas as regiões, enfrentam desafios: 97% das pessoas nas Américas dizem que encontram problemas ao segmentar sua rede. Uma quantidade semelhante disse o mesmo na EMEA (94%) e na APAC (97%).

As empresas da EMEA e da APAC citam a falta de qualificação/conhecimento (38% e 43%) como seu maior obstáculo à segmentação. Para os que estão nas Américas, o maior obstáculo é o aumento dos gargalos de desempenho (41%).

Mais organizações nas Américas consideram suas estruturas de segurança Zero Trust maduras: as pessoas nas Américas têm maior probabilidade de dizer que a implementação do Zero Trust está totalmente concluída e definida (49%) do que na APAC (35%) ou na EMEA (33%).

A segmentação é amplamente reconhecida como parte importante do Zero Trust

Nossos entrevistados concordam que a segmentação é importante para garantir a segurança de suas organizações, principalmente no que se refere ao combate ao malware. Em todos os setores, 93% acreditam que é fundamental ajudar a impedir ataques prejudiciais, um número que sobe para 99% para os setores de manufatura e produção. Isso pode ser devido ao fato de que esses setores dependem muito de vários terceiros em sua cadeia de suprimentos, de modo que uma interrupção pode ter efeitos maciços em cascata nos negócios.

A segmentação também contribui muito para uma estrutura Zero-Trust. Ao citar o motivo pelo qual a organização iniciou um projeto de segmentação, a terceira resposta mais comum foi o avanço do Zero Trust: quase todos os que fizeram alguma segmentação estão implantando ou já implantaram uma estrutura de segurança Zero Trust (99%), embora apenas dois em cada cinco (40%) informem que sua estrutura Zero Trust está totalmente definida e completa.

Globalmente, a maioria dos entrevistados deseja ir além e implementar a microssegmentação, que protege as cargas de trabalho dos aplicativos em um nível granular: 89% afirmam que a microssegmentação é, no mínimo, uma alta prioridade, sendo que 34% a consideram sua principal prioridade. Além disso, 97% das equipes de segurança de TI e dos tomadores de decisão informam que ela foi adotada por pelo menos uma minoria de seu setor. Esse número cai para 80% no caso do setor público (excluindo o setor de saúde), uma diferença que pode ser atribuída a orçamentos mais apertados e à infraestrutura herdada, que representam maiores obstáculos à implementação da proteção em nível de carga de trabalho da microssegmentação.

Microssegmentação

das equipes de segurança de TI e dos tomadores de decisão relatam que a microssegmentação foi adotada por pelo menos uma minoria de seu setor

Mas o setor público pode se beneficiar muito com a implementação de técnicas avançadas de segurança, como a microssegmentação. Como os sistemas desse setor não são necessariamente projetados para interagir uns com os outros, eles não têm interoperabilidade, o que aumenta a probabilidade de erro humano e a probabilidade de um ataque cibernético bem-sucedido.

No nível da segmentação, 15% dos entrevistados do setor público relatam não ter nenhuma segmentação, embora 93% reconheçam sua importância. Isso representa o menor nível de implementação por setor, sendo que o maior obstáculo são os requisitos de conformidade (52%).

A segmentação é boa. A microssegmentação é melhor.

A segmentação é uma abordagem arquitetônica que divide uma rede em segmentos menores com o objetivo de melhorar o desempenho e a segurança.

A microssegmentação divide uma rede em segmentos no nível da carga de trabalho individual, de modo que os controles de segurança e o fornecimento de serviços possam ser definidos para cada segmento exclusivo.

As implementações são lentas, mas a perseverança produz resultados transformadores

A dura realidade é que, mesmo com um consenso tão amplo de que a segmentação é a chave para impedir os ataques, a implantação da segmentação tem sido lenta — mais lenta do que talvez fosse esperado. Apenas 30% das organizações segmentaram mais de duas áreas críticas de negócios em 2023 (em comparação com 25% em 2021), e 44% iniciaram um projeto de segmentação de rede há dois ou mais anos, o que sugere que os esforços foram interrompidos.

As implementações lentas são mais claramente explicadas pelos principais obstáculos encontrados pelos entrevistados: falta de qualificação/conhecimento para segmentação (39%), aumento dos gargalos de desempenho (39%) e requisitos de conformidade (38%; Figura 4). Quase todos os que sobreviveram, independentemente do setor, indústria ou país, reportaram os mesmos obstáculos em medidas ligeiramente diferentes. Vale a pena observar que, embora a falta de qualificação/conhecimento seja a principal causa de atraso nos projetos de segmentação, há uma escassez de talentos em toda a área de cibersegurança e, com as mudanças nesse espaço ocorrendo tão rapidamente, as lacunas de habilidades estão fadadas a existir.

Apesar do progresso lento, as taxas de segmentação estão aumentando gradualmente em geral. A porcentagem de organizações com aplicativos/dados críticos para os negócios segmentados aumentou 12% e os servidores segmentados aumentaram 8% de 2021 a 2023.

Obstáculos encontrados ao segmentar a rede

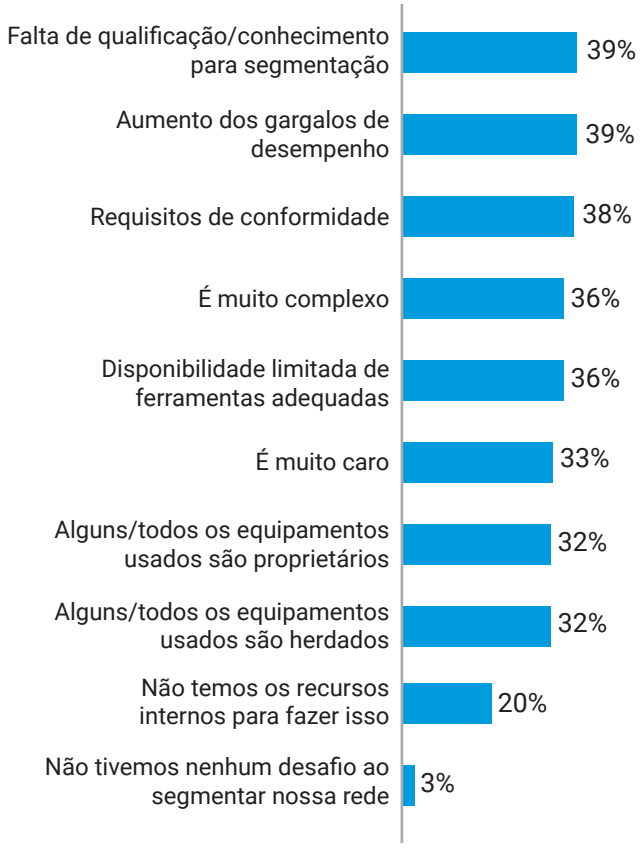

Fig. 4: quais problemas, se houver, sua organização encontrou/prevê ao segmentar a rede? [1.187], mostrado apenas para aqueles que segmentaram sua rede em algum momento, não exibe todas as opções de resposta.

A conclusão: a segmentação de seis áreas críticas de negócios reduz enormemente os riscos

Proteger e segmentar mais ativos imediatamente torna as organizações mais seguras. As equipes de segurança são mais capazes de identificar ataques e podem responder com muito mais eficiência. A implementação de estratégias de segmentação imaturas ou mal definidas provavelmente só aumenta o risco de uma organização, mas, quando bem feita, a segmentação claramente vale tudo o que é necessário para superar os obstáculos e implementá-la.

Nossas descobertas mostram que, após uma violação, a recuperação é 11 horas mais rápida com a segmentação. Fazendo as contas: para aqueles que implementaram a segmentação em seis áreas de missão crítica, são necessárias, em média, quatro horas para interromper completamente um ataque de ransomware; para aqueles com segmentação contra apenas um ativo, são 15 horas.

Da mesma forma, a segmentação economiza 11 horas ao limitar o movimento lateral. Para aqueles que implementaram a segmentação em todas as seis áreas de missão crítica, são necessárias, em média, três horas para limitar significativamente o movimento lateral de um ataque de ransomware. Para aqueles com segmentação em relação a apenas um ativo, a média é de 14 horas.

Considere a diferença que 11 horas fazem para a sua equipe e para a contenção de custos e danos à marca em qualquer cenário.

Para interromper um ataque

4 horas

O tempo que leva, em média, para interromper completamente um ataque de ransomware — para aqueles que segmentaram todos os seis ativos comerciais

Para aqueles que segmentaram apenas um ativo: **15 horas**

Para limitar o movimento

3 horas

O tempo que leva, em média, para limitar significativamente o movimento lateral de um ataque de ransomware — para aqueles que segmentaram todos os seis ativos comerciais

Para aqueles que segmentaram apenas um ativo: **14 horas**

Como uma solução de microssegmentação baseada em software ajuda a resolver desafios

A microssegmentação não apenas permite um tipo de segmentação mais avançado e granular, mas também facilita a implementação.

As soluções baseadas em software, como a Akamai Guardicore Segmentation, podem ser implantadas rapidamente sem a necessidade de fazer alterações físicas na rede. Não há necessidade de mudar o IP de seus novos segmentos ou de se preocupar com a localização física de seus servidores e dispositivos. Isso torna a solução muito mais rápida e fácil de implementar do que as abordagens baseadas em infraestrutura, como firewalls e VLANs. E como a solução usa seu próprio driver proprietário para a aplicação de políticas, ela funciona perfeitamente em máquinas e sistemas operacionais: de servidores bare-metal a implementações em várias nuvens, de tecnologia legada como o Windows Server 2003 aos mais recentes dispositivos IoT/OT e tecnologia em contêineres. Isso significa que você está gerenciando apenas uma única solução com uma interface para visualizar e controlar as conexões feitas por diferentes sistemas operacionais e dispositivos em todo o seu ambiente, independentemente da localização física.

Como isso facilita a implementação

A microssegmentação primeiro gera um visual interativo de todas as conexões que estão sendo feitas em seu ambiente, o que é um componente essencial para superar os principais obstáculos à implementação. Além disso, a Akamai incorporou na solução maneiras ativas de lidar com gargalos de desempenho e requisitos de conformidade.

Os gargalos de desempenho não surgem necessariamente de qualquer tensão técnica em um sistema causada por uma solução de segmentação, mas sim de gargalos na força de trabalho causados pela necessidade de segmentar manualmente as áreas de negócios e, em seguida, solucionar manualmente os problemas dessas áreas quando há falhas. A Akamai trabalha para resolver esse problema, e o principal obstáculo à implantação, a falta de conhecimento, reduzindo a necessidade de segmentação manual e oferecendo suporte técnico e serviços profissionais de alto nível. Nossos especialistas em segmentação fazem parceria com você durante todo o processo de implementação para garantir que suas metas de segmentação em seu ambiente de TI exclusivo sejam alcançadas.

O suporte à implementação também vem da própria solução: suas recomendações de política com tecnologia de IA e modelos de política prontos para uso para casos de uso comuns economizam tempo e cliques, simplificam o fluxo de trabalho, reduzem o tempo total para a política e evitam configurações incorretas devido a erros humanos. Para um de nossos clientes, conseguimos entregar um projeto de segmentação granular estimado em dois anos e mais de US$ 1 milhão em custos totais em apenas seis semanas com um único engenheiro, reduzindo o custo geral do projeto em 85%, provando que a segmentação granular pode ser implementada de forma rápida e fácil, sem sofrer com gargalos.

Como isso facilita a conformidade

Muitos de nossos clientes implementam nossa solução para garantir e atestar a conformidade com várias exigências de conformidade nacionais e internacionais, como PCI-DSS, SWIFT, Sarbanes-Oxley, HIPAA, GDPR e muitas outras. Essas exigências de conformidade geralmente exigem que os dados no escopo sejam separados de outros sistemas em seu ambiente. Embora possa ser proibitivo fazer isso usando firewalls e VLANs, nossa solução baseada em software permite criar segmentos especificamente para dados no escopo e impor regras de comunicação sobre o que pode e o que não pode acessar esses dados. Usando nosso mapa visual com visualizações quase em tempo real e históricas, você pode atestar sua conformidade com essas normas mostrando fisicamente que os dados no escopo não estão sendo acessados por usuários e máquinas não autorizados.

Persista com a solução e o suporte certos para transformar sua postura de segurança

A segmentação pode ser proibitivamente difícil de implementar. Mas, como mostra este relatório, aqueles que conseguem implementá-la de forma eficaz observam reduções maciças em seu risco cibernético. A segmentação adequada limita o movimento lateral das ameaças e permite que você reaja mais rapidamente durante uma violação ativa. E, após uma violação, os esforços de recuperação são seguros e levam menos tempo para serem concluídos.

A escolha de uma solução projetada para superar os desafios comuns da implementação da segmentação — e a parceria com especialistas fornecidos durante essa jornada — coloca você na melhor posição possível para transformar sua postura de segurança. Além disso, quanto mais áreas de negócios você segmenta, mais você também avança em sua arquitetura Zero Trust, reduzindo o risco atual e garantindo uma defesa de primeira linha contra futuros vetores de ameaças.

Nosso grupo de pesquisa

Entrevistamos 1.200 tomadores de decisão de TI e segurança em 10 países para medir o progresso que as organizações fizeram na proteção de seus ambientes, com foco no papel da segmentação.

Foram feitas perguntas relacionadas a suas abordagens de segurança de TI, estratégias de segmentação e ameaças enfrentadas por suas organizações em 2023. Essas descobertas nos deram um insight sobre como as estratégias de segurança mudaram desde 2021, e o quanto ainda precisa ser feito.

Pesquisamos pessoal de segurança e tomadores de decisão dos EUA, México, Brasil, Reino Unido, França, Alemanha, China, Índia, Japão e Austrália. Todos trabalhavam em empresas com mais de 1.000 funcionários e representam uma variedade equilibrada de indústrias e setores.

Nota: essa amostra foi ligeiramente diferente em relação a 2021. Tamanhos de amostras — 2023: 1.200 concluídos, 2021: 1.000 concluídos. Em 2023, os participantes da Austrália, Japão e China também foram entrevistados. Os setores foram ligeiramente diferentes em relação a 2021. Em 2023, nos concentramos especificamente no comércio digital como um setor próprio.

Saiba mais sobre a Akamai Guardicore Segmentation

A Akamai protege a experiência, os sistemas e os dados de seus clientes, ajudando a incorporar a segurança em tudo o que você cria, em qualquer lugar em que o desenvolva e em qualquer lugar em que o entregue. A visibilidade da nossa plataforma em relação às ameaças globais nos ajuda a adaptar e desenvolver sua postura de segurança — para habilitar o Zero Trust, proteger aplicativos e APIs e proteger sua infraestrutura — dando 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 X (antigo Twitter) e no LinkedIn. Publicado em 10/23.

VansonBourne

A Vanson Bourne é uma especialista independente em pesquisa de mercado para o setor de tecnologia. Sua reputação de análises robustas e confiáveis baseadas em pesquisas está fundamentada em princípios rigorosos de pesquisa e em sua capacidade de buscar as opiniões de tomadores de decisão seniores em funções técnicas e comerciais, em todos os setores de negócios e em todos os principais mercados. Para obter mais informações, acesse www.vansonbourne.com.