Akamai

E-BOOK

O estado da segmentação

A superação dos obstáculos de implementação prova ser transformadora

Setor de comércio eletrônico

Índice

Introdução

O trabalho das equipes de segurança de TI, especialmente aquelas que defendem organizações de comércio eletrônico, nunca foi fácil. Tradicionalmente, orçamentos mais apertados e recursos de segurança limitados significam que os defensores corporativos precisam fazer mais com menos. Mas agora, os invasores altamente motivados e sofisticados, combinados com o gerenciamento de uma infræstrutura cada vez mais complexa, estão colocando as equipes de segurança sob maior pressão do que nunca para mitigar riscos. As organizações de comércio eletrônico dependem de uma presença online de alto desempenho para operar, de modo que uma violação bem-sucedida, como um ataque de ransomware, pode causar danos extensos, se não irreparáveis, à reputação da marca e à receita. Imagine o impacto prejudicial se as operações online, o atendimento de pedidos ou as linhas de produção parassem quando servidores e sistemas críticos ficassem indisponíveis devido a um evento de criptografia em massa, e possível dupla extorsão por meio de exfiltração de dados.

Como mostram as descobertas neste relatório "O estado da segmentação" no comércio eletrônico, esses ataques também têm um maior impacto, aumentando as apostas dos líderes na escolha das ferramentas e soluções certas que ajudam a manter os dados críticos seguros, sem sacrificar o desempenho ou adicionar sobrecarga operacional. De acordo com o relatório, o comércio eletrônico é o setor mais visado de todos os participantes da pesquisa, destacando a urgência de prevenir, detectar e responder o mais rápido possível a um ataque de ransomware para conter as consequências.

Os entrevistados nas organizações do setor de comércio eletrônico (representando todas as regiões, incluindo os EUA, América Latina, EMEA e APAC) concordam com a eficácia da segmentação para manter os ativos de TI protegidos, mas o progresso geral na implantação dessa segmentação em torno de aplicativos, servidores e sistemas comerciais críticos é menor do que o esperado. Os principais obstáculos para as organizações de comércio eletrônico têm sido a falta de conhecimento para implantar a segmentação de forma eficaz, juntamente com os requisitos trabalhosos de conformidade de dados. Isso mostra que as equipes não estão apenas lutando para recrutar ou reter os talentos necessários para seu setor, mas também podem achar que um tempo precioso está sendo gasto tentando garantir a conformidade com a legislação, o que consome ainda mais recursos já sobrecarregados.

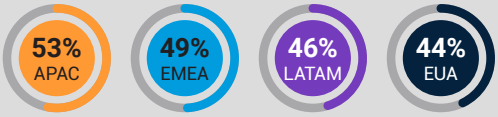
A boa notícia? A perseverança e a escolha da solução certa compensam. Para aqueles que segmentaram com sucesso a maioria de seus ativos críticos em seis áreas principais, a segmentação provou ter um efeito transformador nos recursos defensivos, o que permitiu mitigar e conter ransomware 11 horas mais rapidamente do que aqueles com apenas um ativo segmentado. Imagine a diferença que essas 11 horas podem fazer não apenas para seus responsáveis por resolver incidentes, mas também para seus clientes e para reputação da marca.

A segmentação progrediu lentamente em geral, mas aqueles que perseveram reduziram significativamente seus riscos

A segmentação é boa. A microssegmentação é melhor.

A segmentação é uma abordagem arquitetônica que divide uma rede em segmentos menores para melhorar a segurança e reduzir o risco associado a redes planas. Ela também vem sendo usada para ajudar a reduzir o escopo, o custo e a dificuldade de alcançar e manter a conformidade com o PCI para organizações orientadas por comércio eletrônico.

A microssegmentação é uma técnica de segurança definida por software que divide logicamente uma rede em segmentos de segurança distintos até a carga de trabalho individual ou o nível do processo (Camada 7). Os controles de segurança e a entrega de serviços podem ser definidos para cada segmento exclusivo em um nível mais granular quando comparados aos métodos tradicionais de segmentação, como VLANs, ACLs e firewalls internos, que oferecem apenas o controle da Camada 4. É por isso que 94% dos entrevistados do setor de comércio eletrônico preferem soluções de segmentação baseadas em software em relação aos métodos tradicionais.



Os tomadores de decisões de segurança na APAC têm maior probabilidade do que os da EMEA, LATAM ou dos EUA de dizer que a segmentação de rede é extremamente importante para garantir que sua organização seja segura. Aqueles na América Latina têm maior probabilidade de dizer que a microssegmentação é a prioridade máxima (42%) do que os colegas na APAC (35%), nos EUA (34%), e na EMEA (26%).

O comércio eletrônico é o setor mais visado, e os ataques de ransomware continuam a aumentar

A quantidade de ataques de ransomware em organizações de comércio eletrônico (bem-sucedidos e malsucedidos) foi, em média, de 167 nos últimos 12 meses. Isso não só coloca o comércio eletrônico no topo da lista do número médio de ataques de ransomware, mas esse número também corresponde ao dobro do número do setor mais próximo (média do setor de construção de 89 ataques).

É mais provável que os invasores cibernéticos visem organizações nos EUA: o número de ataques de ransomware nos EUA é o mais alto entre todas as regiões, com 312 ataques em média nos últimos 12 meses, em comparação com 119 na APAC, 91 na EMEA e 68 na América Latina (figura 1).

Número médio de ataques de ransomware em organizações de comércio eletrônico nos últimos 12 meses, por região

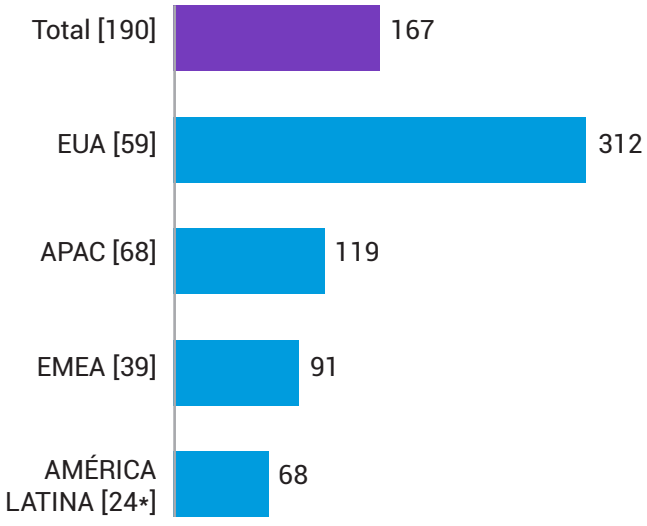


Fig. 1: Quantos ataques de ransomware foram feitos contra sua organização nos últimos 12 meses (independentemente de terem sido bem-sucedidos ou não)? O gráfico mostra o número médio de ataques nos últimos 12 meses, dividido por região. Dados apenas do setor de comércio eletrônico.

*Atenção: o tamanho da base baixa está abaixo de 30

Embora as médias nas regiões fora dos EUA não possam ser descritas como baixas, elas são insignificantes em relação ao número de ataques que se concentram nos EUA. Com a maior economia do mundo, os EUA são o país mais visado por gangues de ransomware, e os invasores frequentemente estão de olho em outros países de língua inglesa e ocidentais. As motivações geopolíticas também afetam os países e setores mais atingidos. As organizações de comércio eletrônico são alvos frequentes porque tradicionalmente têm menos maturidade de segurança quando comparadas a organizações de outros setores, como os de serviços financeiros, tornando-as um alvo mais fácil. Para piorar, um ataque ransomware bem-sucedido pode ser altamente público, especialmente se as organizações forem atingidas durante períodos críticos de geração de receita, como feriados, festivais, eventos esportivos, volta às aulas ou outros eventos de pico de compras, aumentando a probabilidade de um pagamento, na mente do invasor, caso as operações sejam interrompidas.

Apesar do alto número de ataques de ransomware dos quais as organizações de comércio eletrônico estão sendo alvo, há um nível decepcionante de segmentação sendo implementada. Apenas 11% dessas organizações segmentaram mais de duas áreas, um valor amplamente consistente em todas as regiões. Isso indica que muitas dessas organizações podem ter recursos limitados além do que é necessário para lidar com problemas e ataques à medida que eles surgem.

Os ataques de ransomware no setor de comércio eletrônico podem ter impactos enormes e imediatos sobre os negócios (figura 2), com nossos entrevistados indicando perda financeira e danos à reputação, que aumentam significativamente os riscos para as equipes de segurança em organizações de comércio eletrônico. Aumentos também foram observados na proporção de entrevistados que relataram prêmios de seguro mais altos. Isso demonstra o nível de risco que as organizações de comércio eletrônico podem carregar, frequentemente contendo dados pessoais sobre indivíduos e seus hábitos de compra, além dos riscos relacionados a questões logísticas com estoque ou armazenamento.

Os impactos podem variar de acordo com a região: Os entrevistados da APAC são particularmente propensos a destacar perdas financeiras, com mais da metade (51%) indicando isso, em comparação com a média geral de 42%. Os entrevistados dos EUA, no entanto, têm maior probabilidade de relatar o tempo de inatividade da rede, com quase metade (49%) citando isso, em comparação com a média geral de 39%. Os entrevistados da UE têm maior probabilidade de relatar uma redução na moral dos funcionários como um impacto (41%, em comparação com os 36% globalmente).

Também vemos o efeito dessa pressão em termos de estratégia: o número de organizações de comércio eletrônico que estão atualizando continuamente as estratégias ou políticas de cibersegurança aumentou de 3% em 2021 para 13% em 2023, não apenas em resposta ao ransomware, mas também a uma superfície de ataque em constante mudança. O aumento da complexidade da infraestrutura à medida que as cargas de trabalho migram para a nuvem é apenas um dos fatores de risco que afetam as estratégias de segurança e as equipes de segurança diariamente.

Impacto de ransomware/ataques cibernéticos em organizações de comércio eletrônico

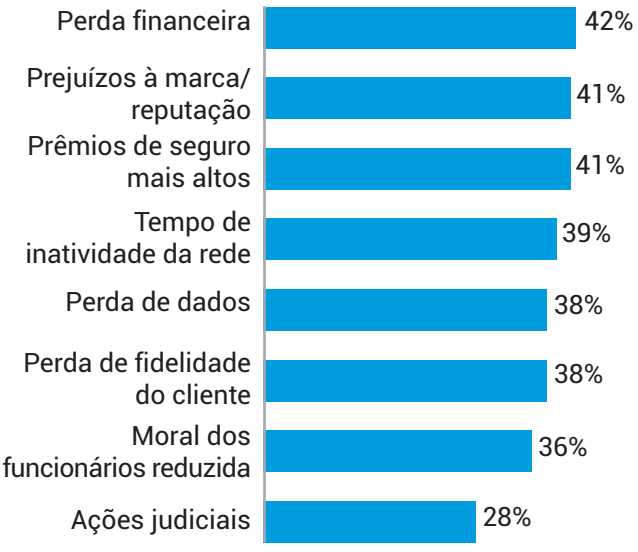
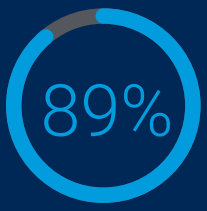


Fig. 2: Quando sua organização detectou anteriormente ransomware ou algum outro ataque cibernético, qual dos seguintes impactos sua organização sofreu? O gráfico não mostra todas as opções de resposta, somente dados do setor de comércio eletrônico.

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, e principalmente no que se refere ao combate ao malware.



Quase metade (48%) afirma que a segmentação é extremamente importante, e 89% acreditam que é essencial ajudar a impedir ataques prejudiciais.

A segmentação também é reconhecida como uma base de uma estrutura de segurança Zero Trust, e a boa notícia para as organizações de comércio eletrônico é que já foram feitos progressos nessa área. Todos estão implantando ou já implantaram uma estrutura de segurança Zero Trust (100%), embora apenas mais de dois em cinco (42%) relatem que sua estrutura Zero Trust está totalmente completa e definida e pode ser considerada madura. Portanto, essa é uma área em que a segmentação pode ajudar as organizações de comércio eletrônico a avançar em sua jornada rumo ao Zero Trust. Com base nos dados, as organizações nos EUA estão muito mais maduras quando se trata de sua implantação de estrutura de segurança Zero Trust: Elas têm muito mais probabilidade de dizer que sua implantação Zero Trust está totalmente completa e definida (63%), em comparação com a América Latina (46%), APAC (32%) e EMEA (23%).

Os motivos para iniciar um projeto de segmentação de rede variaram significativamente por região, com um foco do governo na cibersegurança subindo ao topo com 41%. A América Latina e os países da UE listaram vulnerabilidades de dia zero de alto perfil como os principais motivadores para a busca de uma iniciativa de segmentação (44% e 42%, respectivamente). Mas os entrevistados na UE são muito mais propensos a informar também que os projetos começaram porque é uma prática recomendada (41%, em comparação com os 22% globais). No entanto, os entrevistados dos EUA e da região Ásia-Pacífico têm maior probabilidade de dizer que começaram por causa do foco do governo em cibersegurança (41% e 39%, respectivamente, em comparação com os 35% globais). Os entrevistados da região Ásia-Pacífico também têm maior probabilidade de dizer que a migração de aplicativos críticos para a nuvem foi o que os fez iniciar um projeto (39%, em comparação com os 32% globais).

A maioria dos entrevistados nas organizações de comércio eletrônico deseja ir além e implementar a microssegmentação, que protege as cargas de trabalho dos aplicativos em um nível granular: 92% afirmam que a microssegmentação é, no mínimo, uma alta prioridade, sendo que 34% a consideram sua principal prioridade. Além disso, todos (100%) os tomadores de decisões de TI e segurança nesse setor relatam que a microssegmentação foi adotada por pelo menos uma minoria de seu setor, enfatizando que é uma solução que, pelo menos, gera ampla conscientização nas pessoas, mesmo que os progressos tenham sido limitados até o momento.

Os entrevistados também observaram que era necessário obter mais visibilidade no ambiente de TI das organizações. Aqueles que estão na América Latina afirmam que precisam de "muito mais" visibilidade (63%) — seguidos pela APAC (56%), EUA (46%) e EMEA (44%) — das comunicações de rede, locais de ativos etc., para reduzir riscos.

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 protegendo os ativos de TI, a implantação da segmentação tem sido lenta — talvez mais lenta do que o esperado.

Apenas 11% das organizações de comércio eletrônico segmentaram mais de duas áreas críticas de negócios, e 48% iniciaram pela primeira vez um projeto de segmentação de rede há dois ou mais anos, o que sugere que os esforços foram interrompidos.

As áreas de missão crítica

- Aplicativos críticos
- Aplicativos voltados para o público
- Controladores de domínio
- Pontos de extremidade
- Servidores
- Ativos/dados críticos para os negócios

As implementações lentas são mais claramente explicadas pelos principais obstáculos encontrados pelos entrevistados: falta de qualificação/conhecimento para segmentação (40%), requisitos de conformidade (40%) e aumento dos gargalos de desempenho (38%). Todos associados com os métodos de segmentação tradicionais. Vale a pena observar que, embora a falta de recursos ou 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.

As organizações de comércio eletrônico, em todas as regiões, enfrentam desafios: 100% das pessoas nos EUA e na América Latina dizem que encontram problemas ao segmentar sua rede. Quase a mesma quantidade disse o mesmo na APAC (99%) e na EMEA (97%).

No entanto, quando distribuído por região (figura 3), há variação nos obstáculos mais prováveis de serem encontrados. Isso mostra que certos problemas (por exemplo, falta de habilidades, conformidade) podem ser motivados tanto quanto ou mais por questões locais do que por questões globais.

As empresas da EMEA e da LATAM citam a falta de qualificação/conhecimento (ambas com 54%) como seu maior desafio para a segmentação. Para empresas nos EUA, o maior desafio é o aumento dos gargalos de desempenho (44%) e, na APAC, o problema provavelmente são os requisitos de conformidade (43%).

	O problema mais provável	Segundo e terceiro problemas mais prováveis	
EUA [59]	Aumento dos gargalos de desempenho (44%)	Requisitos de conformidade/disponibilidade limitada de ferramentas apropriadas (ambos 41%)	
AMÉRICA LATINA [24*]	Falta de qualificação/conhecimento para segmentação (54%)	É muito complexo (46%)	Alguns ou todos os equipamentos usados são patenteados/Alguns ou todos os equipamentos usados são legados (ambos 38%)
EMEA [39]	Falta de qualificação/conhecimento para segmentação (54%)	Disponibilidade limitada de ferramentas adequadas (41%)	Requisitos de conformidade/Alguns ou todos os equipamentos usados são legados /É muito caro (todos 36%)
APAC [67]	Requisitos de conformidade (43%)	Disponibilidade limitada de ferramentas adequadas/Alguns ou todos os equipamentos usados são patenteados/Maiores gargalos de desempenho (todos 37%)	

Fig. 3: Quais problemas, se houver, sua organização encontrou/prevê ao segmentar a rede? O gráfico mostra aqueles que segmentaram sua rede em algum momento, mostrando as três principais respostas selecionadas por região, dados somente do setor de comércio eletrônico.

*Atenção: o tamanho da base baixa está abaixo de 30

Principais conclusões: Aqueles que segmentaram seis áreas críticas de negócios reduziram os riscos significativamente

Proteger e segmentar mais ativos no ambiente de comércio eletrônico imediatamente torna as organizações mais seguras. Com a solução certa, as equipes de segurança conseguem identificar ataques mais rapidamente, melhorando assim o tempo médio de detecção (MTTD) e o tempo médio de resposta (MTTR) a um incidente. No entanto, a subsegmentação de ativos, geralmente resultado do uso de tecnologias de segmentação legadas, pode criar lacunas e pontos cegos na segurança, deixando a organização em uma posição mais vulnerável ou reativa. Mas, quando feita corretamente, a segmentação por meio de uma abordagem definida por software pode ajudar as organizações a gerenciar melhor suas superfícies de ataque para manter os ativos críticos protegidos de maneira mais eficiente e econômica.

Nossas descobertas mostram que, após uma violação, a recuperação é 11 horas mais rápida com a segmentação. Fazendo as contas: Para as organizações de comércio eletrônico que implementaram segmentação em seis áreas de missão crítica, leva em média três horas para interromper completamente um ataque de ransomware. Para aqueles com segmentação em relação a apenas um ativo, a média é de 14 horas.

Da mesma forma, a segmentação economiza 11 horas para a contenção do 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 para a sua equipe, os danos à marca e o custo incorridos durante essas 11 horas, em qualquer um dos cenários.

Para interromper um ataque

3 horas

O tempo que leva, em média, para interromper completamente um ataque de ransomware, para aqueles que segmentaram os seis ativos de negócios. Para aqueles que segmentaram apenas um ativo: **14 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 os seis ativos de negócios. 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 o 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 infræstrutura, como firewalls e VLANs. E como a solução não depende do sistema de operação subjacente para a aplicação de políticas, ela funciona perfeitamente em máquinas e sistemas operacionais: de servidores bare metal a implementações multinuvem, de tecnologia legada como o Windows Server 2003 e o Windows XP aos mais recentes sistemas de POV, 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

O Akamai Guardicore Segmentation 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 de gargalos na força de trabalho. Quando algo é danificado, pode ser necessário dedicar muito tempo e esforço para segmentar manualmente as áreas de negócios e, em seguida, solucionar manualmente os problemas nessas áreas. A Akamai trabalha para resolver esse problema (e o principal obstáculo à implantação, a falta de conhecimento) reduzindo o tempo gasto com a 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 rotulagem e política alimentadas por 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 implementação de políticas 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 a segmentação otimiza a conformidade

Muitos de nossos clientes implementam nossa solução para garantir e atestar a conformidade com várias exigências de conformidade específicas do país e internacionais, como PCI DSS, SWIFT, Sarbanes-Oxley, HIPAA, GDPR e muitas outras. Esses requisitos de conformidade geralmente exigem que os dados no escopo, como o ambiente de dados de titulares de cartão (CDE) para o PCI DSS, sejam separados e protegidos 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 conformidade com normas mostrando fisicamente que os dados no escopo não estão sendo acessados por usuários, sistemas 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. Ter uma segmentação adequada em funcionamento limita o movimento lateral e permite que os responsáveis por resolver incidentes reajam mais rapidamente durante um ataque ativo. E, após uma violação, os esforços de recuperação são seguros e levam menos tempo para serem concluídos.

A escolha de uma solução definida por software projetada para superar os desafios comuns associados com a implementação da segmentação tradicional, e a parceria com especialistas fornecidos durante essa jornada, colocam você na melhor posição possível para transformar sua postura de segurança. Além disso, quanto mais áreas de negócios você segmenta, mais você avança em sua arquitetura Zero Trust, reduzindo o risco atual.

Nosso grupo de pesquisa

Para os fins deste relatório, analisamos 190 entrevistados que trabalham no setor de comércio eletrônico (59 nos EUA, 39 na EMEA, 68 na APAC e 24 na América Latina).

Para o estudo de pesquisa completo, 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. Esses insights e descobertas nos deram informações sobre como as estratégias de segurança mudaram desde 2021, e onde ainda é necessário progredir.

Os entrevistados foram pesquisados em todo o mundo, incluindo os dos EUA, Índia, México, Brasil, Reino Unido, França, Alemanha, China, Japão e Austrália. Eles eram colaboradores de organizações com mais de 1.000 funcionários e de diversos setores e indústrias.

Nota: Essa amostra foi ligeiramente diferente em relação a 2021. Tamanhos da amostra: 2023: 1.200 concluídas, 2021: 1.000 concluídas. 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 o Akamai Guardicore Segmentation

A Akamai protege sua experiência do cliente, sua força de trabalho, seus sistemas e seus dados ajudando a incorporar a segurança em tudo o que você criar, em qualquer lugar que você criar e entregar. A visibilidade da nossa plataforma em relação às ameaças globais nos ajuda a adaptar e desenvolver sua postura de segurança para permitir Zero Trust, interromper ransomware, proteger aplicações e APIs ou combater ataques DDoS, dando a você a confiança para inovar, expandir e transformar continuamente o que é possível. Saiba mais sobre as soluções de computação em nuvem, segurança e entrega de conteúdo da Akamai em akamai.com e www.akamai.com/blog, ou siga a Akamai Technologies no X, antigo Twitter, e LinkedIn. Publicado em 05/24.

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.