E-BOOK

Como superar obstáculos de implantação para proteger sistemas bancários críticos

Relatório de estado global da segmentação

Índice

Introdução

A proteção do setor de serviços financeiros sempre representou desafios significativos e exclusivos para as equipes de segurança de TI. No entanto, invasores cada vez mais sofisticados agora estão combinando técnicas para lançar ameaças maiores e mais frequentes, colocando as equipes de segurança de instituições de serviços financeiros sob uma pressão maior do que nunca. As instituições de serviços financeiros dependem de uma presença digital para operarem, logo, 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 comprometer o desempenho geral ou colocar em risco a exposição de grandes quantidades de dados confidenciais.

Os entrevistados em instituições de serviços financeiros (representando todas as regiões, incluindo os EUA, América Latina, EMEA e APAC) concordam majoritariamente com a eficácia da segmentação para manter os ativos protegidos, mas o progresso geral na implantação em torno de aplicativos e ativos de negócios críticos é menor do que o esperado. O principal obstáculo para as instituições de serviços financeiros tem sido o aumento dos gargalos, o que sugere que as equipes podem estar reagindo às ameaças sem ter tempo ou apoio para entender e mitigar completamente os impactos no desempenho resultantes das mudanças.

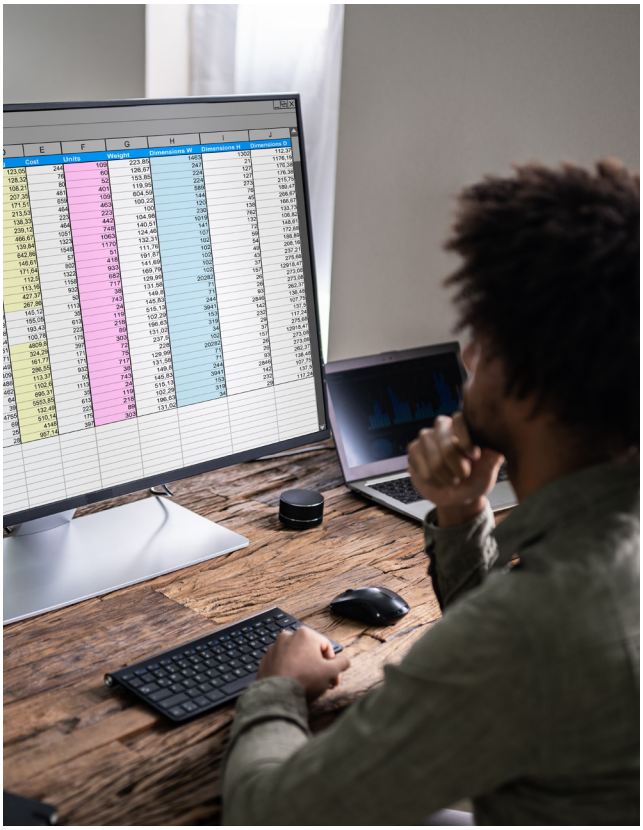
A boa notícia? A perseverança compensa. A segmentação provou ter um efeito transformador na defesa para aqueles que segmentaram a maioria de seus ativos essenciais, permitindo que eles mitigassem e contivessem o ransomware 13 horas mais rápido do que aqueles com apenas um ativo segmentado. Imagine a diferença que essas 13 horas fazem para sua equipe, clientes e reputação.

O resultado: a segmentação progrediu lentamente em geral, mas aqueles que perseveraram reduziram imensamente o risco.

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 é uma técnica de segurança que permite dividir logicamente uma rede em segmentos de segurança distintos até o nível de carga de trabalho individual. Os controles de segurança e a prestação de serviços podem então ser definidos para cada segmento exclusivo.



Os ataques de ransomware continuam aumentando, assim como seu impacto

O número de ataques de ransomware em instituições de serviços financeiros (bem-sucedidos e malsucedidos) aumentou em quase 50% nos últimos dois anos, de 43 em média em 2021 para 62 em 2023. Apesar da reputação que o setor possui de ter medidas de segurança sólidas, esses números ressaltam uma vulnerabilidade crítica que não pode ser ignorada. É evidente que o setor de serviços financeiros não está imune à ameaça de ransomware, e a complacência não é uma opção.

As instituições de serviços financeiros na região da APAC foram alvo do maior número de ataques de ransomware em média (73), e a América Latina apresentou os números mais baixos (48, figura 1).

Número médio de ataques de ransomware no setor de serviços financeiros nos últimos 12 meses por região

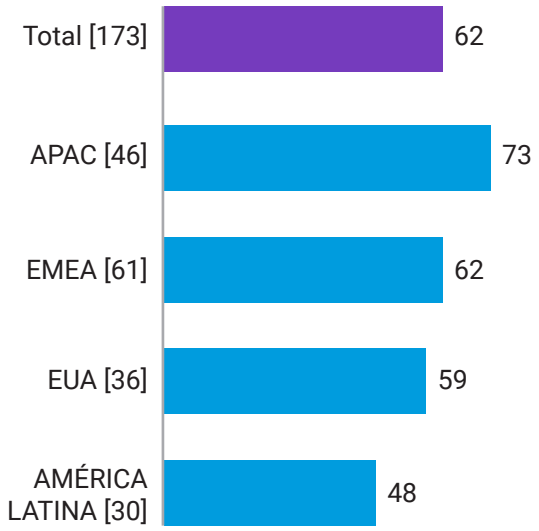


Fig. 1: quantos ataques de ransomware foram feitos contra sua organização nos últimos 12 meses (independentemente de terem sido bem-sucedidos ou não)? O gráfico mostra o número médio de ataques nos últimos 12 meses dividido por região (números base mostrados), apenas dados do setor de serviços financeiros.

Como a maioria das instituições de serviços financeiros opera globalmente, o aumento do número de ataques direcionados na APAC pode resultar da percepção dos hackers de que os alvos da APAC oferecem rendimentos mais altos. No entanto, isso não significa que as instituições financeiras de outras regiões são mais seguras, apenas que elas podem ter maior probabilidade de sofrer ataques laterais que se originam em outro lugar.

Além disso, os entrevistados na América Latina têm maior probabilidade de dizer que a instituição financeira deles segmentou mais de dois ativos, seguidos pela APAC. Isso mostra que as instituições financeiras da APAC podem estar tentando aumentar sua segmentação em razão do número de ataques de ransomware que estão sendo direcionados a elas.

Quem segmentou mais de dois ativos/área por região no setor de serviços financeiros

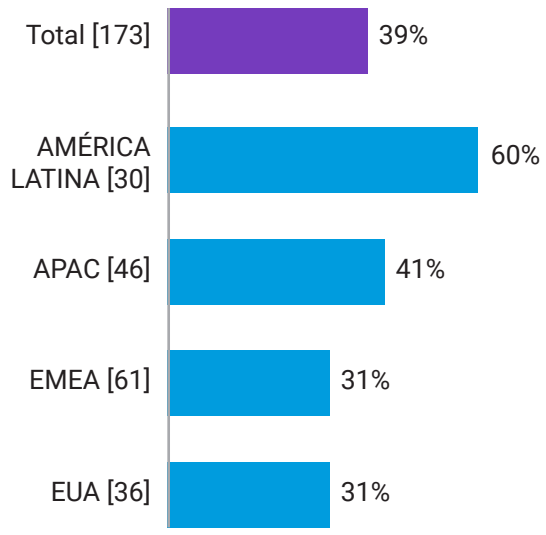


Fig. 2: para cada uma das seguintes medidas de segurança de TI, quais ativos, se houver, estão sendo cobertos? O gráfico mostra apenas as respostas para a medida de segurança de segmentação e as porcentagens que estão usando segmentação para proteger os ativos principais, divididas por região (números base mostrados), apenas dados do setor de serviços financeiros.

Os ataques de ransomware não apenas ocorreram com mais frequência em 2023 do que em 2021, mas seus impactos foram mais bem-sucedidos (figura 3), com nossos entrevistados indicando aumentos no tempo de inatividade da rede e na perda de dados, o que aumenta significativamente os riscos para as equipes de segurança. Também foram observados aumentos na proporção de entrevistados que relataram maiores prêmios de seguro, impulsionados especialmente pelos entrevistados dos EUA (56%). Isso demonstra o nível de risco que as instituições financeiras podem representar, muitas vezes mantendo dados não apenas sobre os indivíduos, mas também sobre as empresas.

Vemos o efeito dessa pressão também em termos de estratégia: o número de instituições de serviços financeiros que estão atualizando continuamente as estratégias ou políticas de cibersegurança aumentou de 3% em 2021 para 18% em 2023, não apenas em resposta ao ransomware, mas também a uma superfície de ataque em constante mudança. Forças de trabalho e aplicativos distribuídos e dados migrando para a nuvem são apenas dois fatores que afetam a estratégia de segurança diariamente.

Impacto de ransomware/ataques cibernéticos em instituições de serviços financeiros

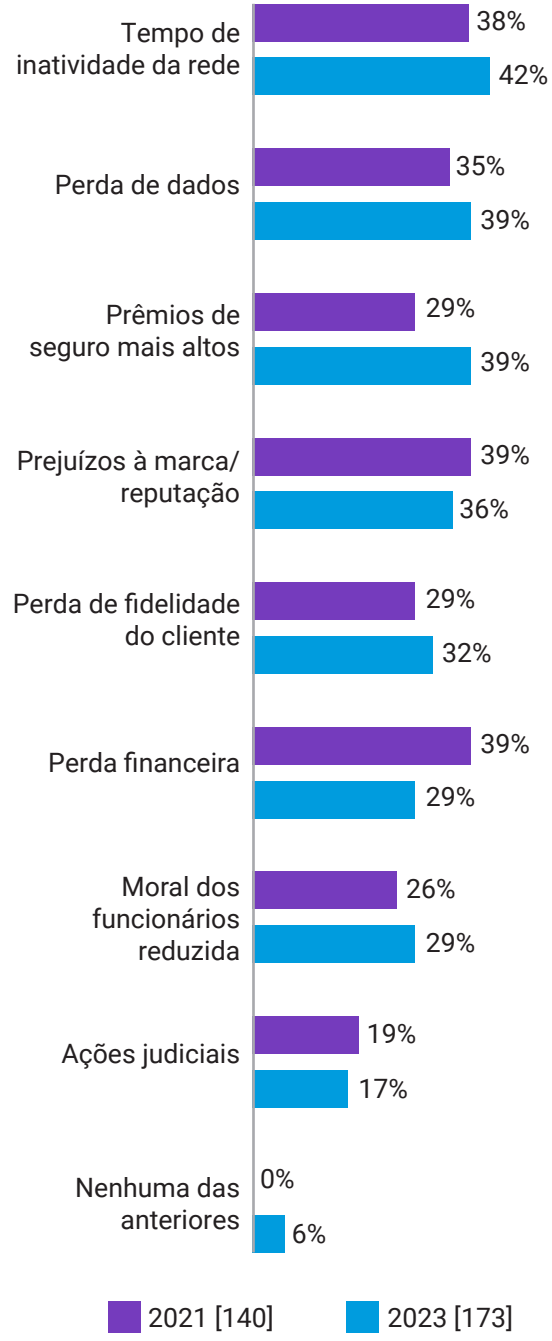


Fig. 3: quando sua organização detectou anteriormente ransomware ou algum outro ataque cibernético, quais dos seguintes impactos isso teve em sua organização? O gráfico mostra os tamanhos da base por ano, divididos por dados históricos, apenas dados do setor de serviços financeiros, e não são mostradas todas as opções de resposta.

A segmentação é o pilar do Zero Trust

Nossos entrevistados no setor de serviços financeiros concordam que a segmentação é importante para garantir a segurança de suas organizações, e principalmente no que se refere ao combate ao malware: 66% afirmam que ela é extremamente importante, e 92% acreditam que é essencial para ajudar a impedir ataques prejudiciais.

A segmentação também contribui muito para uma estrutura Zero Trust. Ao citar por que a organização começou um projeto de segmentação, a resposta mais comum foi avançar no Zero Trust: quase todos aqueles que segmentaram estão implantando ou já implantaram uma estrutura de segurança Zero Trust (99%), embora menos da metade (47%) relate que essa estrutura está totalmente completa e definida e, portanto, madura.

A maioria dos entrevistados nas instituições de serviços financeiros deseja ir além e implementar a microssegmentação, que protege as cargas de trabalho dos aplicativos em um nível granular: 88% afirmam que a microssegmentação é, no mínimo, uma alta prioridade, sendo que 39% a consideram sua principal prioridade. Os entrevistados na América Latina têm maior probabilidade de considerar isso como uma prioridade máxima (50%), sendo que aqueles na região EMEA são os menos propensos (31%). O fato de que os entrevistados da América Latina têm mais probabilidade de relatar que essa é uma prioridade principal se reflete em seu desempenho (figura 1), mostrando que as organizações que priorizam a microssegmentação podem esperar colher os benefícios.

Além disso, 99% dos tomadores de decisões de TI nesse setor relatam que a microssegmentação foi adotada por pelo menos uma minoria de seu setor, enfatizando que é uma solução da qual quase todos têm amplo reconhecimento.

A perseverança gera 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 39% das instituições de serviços financeiros segmentaram mais de duas áreas críticas de negócios em 2023 (em comparação com 26% em 2021), e 45% iniciaram pela primeira vez um projeto de segmentação de rede há dois ou mais anos, o que sugere que os esforços foram interrompidos.

As implantações lentas são explicadas com mais clareza pelos principais obstáculos encontrados pelos entrevistados: aumento dos gargalos de desempenho (41%), falta de habilidades/conhecimento para segmentação (39%) e requisitos de conformidade (35%). Vale a pena observar que, embora a falta de capacitação ou de 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.

No entanto, quando é feita a distribuição por região (veja a figura 4), há variação nos obstáculos mais prováveis de serem encontrados. Isso mostra que certos problemas podem ser impulsionados tanto, se não mais, por condições locais (por exemplo, falta de habilidades nos EUA, preocupações de conformidade na APAC) quanto por questões globais.

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 17% e os servidores segmentados também aumentaram 17% de 2021 a 2023. Esses aumentos superam os aumentos médios globais observados em todos os setores (12% e 8%, respectivamente), mostrando que os departamentos de TI nas instituições de serviços financeiros são um pouco mais capazes do que a maioria de lidar com obstáculos encontrados. Isso pode acontecer porque os requisitos de conformidade geralmente rígidos mencionados acima exigem um nível de segurança cada vez mais forte. Também pode haver relação com os prêmios de seguro mais altos que as instituições de serviços financeiros estão enfrentando. As seguradoras podem estar impondo requisitos para que seus clientes possam resolver certos problemas o mais rápido possível.

Obstáculos encontrados durante a segmentação da rede no setor de serviços financeiros: três principais por região

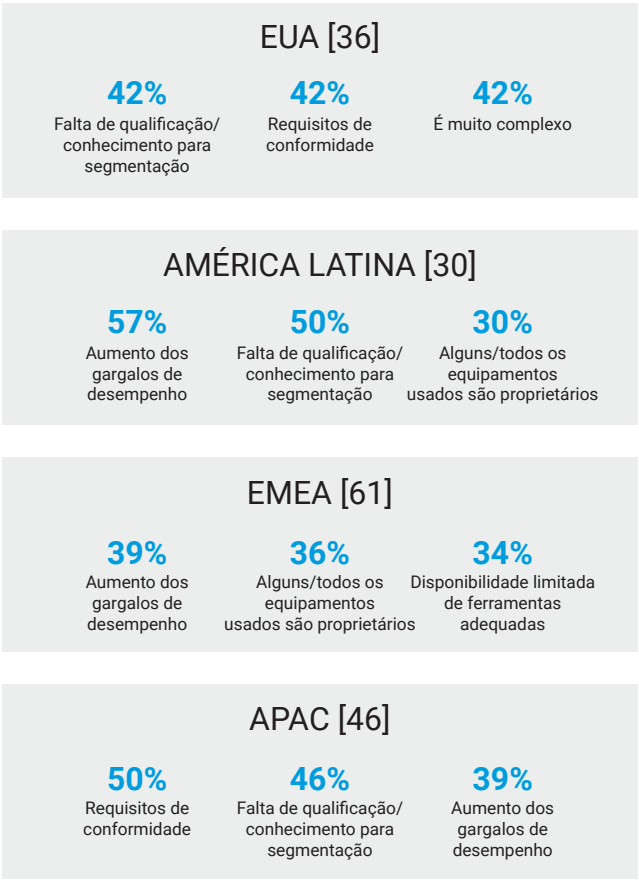


Fig. 4: quais problemas, se houver, sua organização encontrou/prevê ao segmentar a rede? O gráfico mostra os tamanhos de base por região, pergunta mostrada apenas para quem segmentou sua rede em algum momento, mostrando apenas as três principais respostas selecionadas por região, apenas dados do setor de serviços financeiros.

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

Proteger e segmentar mais ativos imediatamente torna as instituições financeiras 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 só aumenta a vulnerabilidade.

No entanto, quando feita corretamente, a segmentação melhora a resiliência cibernética e impede que os ataques cibernéticos causem falhas importantes nos negócios, impedindo que ransomware e violações se espalhem para sistemas e dados críticos.

Nossas descobertas mostram que, após uma violação, a recuperação é 13 horas mais rápida com a segmentação.
Fazendo as contas: para as instituições de serviços financeiros 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 para apenas um ativo, a média é de 16 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 os custos incorridos durante essas 11 a 13 horas, dependendo do cenário.

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: **16 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

As instituições financeiras estão buscando melhorar a escalabilidade, aproveitar os investimentos existentes, otimizar custos e melhorar a agilidade e a flexibilidade migrando cargas de trabalho para a nuvem, muitas vezes integrando data centers locais com nuvens públicas ou privadas. As soluções de segmentação definidas por software, como o Akamai Guardicore Segmentation, surgiram como uma abordagem flexível, simplificada e econômica para a segurança no nível do aplicativo, acelerando drasticamente a implementação, simplificando a manutenção e mitigando efetivamente as ameaças. Como é mais rápida e fácil de implantar do que abordagens baseadas em infraestrutura, como firewalls e VLANs, a solução permite que as instituições financeiras alcancem a segurança em escala, ao mesmo tempo em que atendem às demandas aceleradas de seus negócios e proporcionam experiências inovadoras aos clientes com tecnologias de ponta. Além disso, ela opera perfeitamente em diversos sistemas e ambientes, fornecendo gerenciamento e controle centralizados, de servidores bare metal a implantações multinuvem e sistemas legados. Dessa forma, oferece uma solução unificada para visualizar e controlar conexões em todo o 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 a microssegmentação facilita a conformidade

Muitos de nossos clientes implementam nossa solução para garantir e atestar a conformidade com várias exigências de conformidade, como PCI DSS, SWIFT, Sarbanes-Oxley, GDPR, DORA e muitas outras. Esses requisitos regulatórios 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 complexa. Mas, como mostra este relatório, quem consegue implementá-lo com eficiência pode ver segurança de rede aprimorada, melhor desempenho de rede, conformidade e gerenciamento de rede simplificado. 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.

Conclusões regionais

A segmentação e a microssegmentação são mais importantes na EMEA e nos EUA do que na América Latina: os tomadores de decisão de segurança de TI na EMEA (70%) e nos EUA (60%) têm maior probabilidade de dizer que a segmentação da rede é extremamente importante para garantir a segurança da organização do que os da América Latina (57%).

As pessoas na América Latina têm maior probabilidade de dizer que a microssegmentação é a prioridade principal: (50%) em relação aos colegas nos EUA (42%), APAC (41%) e EMEA (31%).

É mais provável que as empresas da EMEA não tenham feito nenhuma segmentação: É mais provável que as pessoas na EMEA digam que nenhum ativo crítico para os negócios foi segmentado (7%). Todas as outras regiões haviam feito segmentação até certo ponto.

É mais provável que as empresas na América Latina tenham feito o maior progresso com a segmentação: é mais provável que as organizações de serviços financeiros da América Latina tenham segmentado mais de dois ativos essenciais aos negócios (60%) do que as da APAC (41%), da EMEA (31%) e dos EUA (31%).

As organizações, em todas as regiões, enfrentam desafios: 98% das empresas da APAC dizem que encontram problemas ao segmentar a rede, e uma porcentagem semelhante disse o mesmo nos EUA (97%), embora um pouco menos tenha dito isso na EMEA (89%) e na América Latina (87%).

As instituições de serviços financeiros na América Latina são muito mais maduras quando se trata de implantação de estrutura de segurança Zero Trust: essas instituições na América Latina têm muito mais probabilidade de dizer que sua implantação Zero Trust está totalmente completa e definida (57%), em comparação com a EMEA (48%), os EUA (47%) e a APAC (41%).

Nosso grupo de pesquisa

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.

Foram entrevistadas pessoas de todo o mundo, incluindo dos EUA, Índia, México, Brasil, Reino Unido, França, Alemanha, China, Japão e Austrália. Elas eram de organizações com mais de 1.000 funcionários e de diversos setores e indústrias.

Para efeitos deste relatório, foram analisados 173 (2023) e 140 (2021) entrevistados no setor de serviços financeiros.

Saiba mais sobre Akamai Guardicore Segmentation

A Akamai potencializa e protege a vida online. As principais empresas do mundo escolhem a Akamai para criar, entregar e proteger suas experiências digitais, ajudando bilhões de pessoas a viver, trabalhar e se divertir todos os dias. 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 aplicativos 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 da Akamai para instituições financeiras em akamai.com/finserv e akamai.com/blog, ou siga a Akamai Technologies no X, antigo Twitter, e no LinkedIn. Publicado em 05/24.

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 mais informações, visite www.vansonbourne.com.