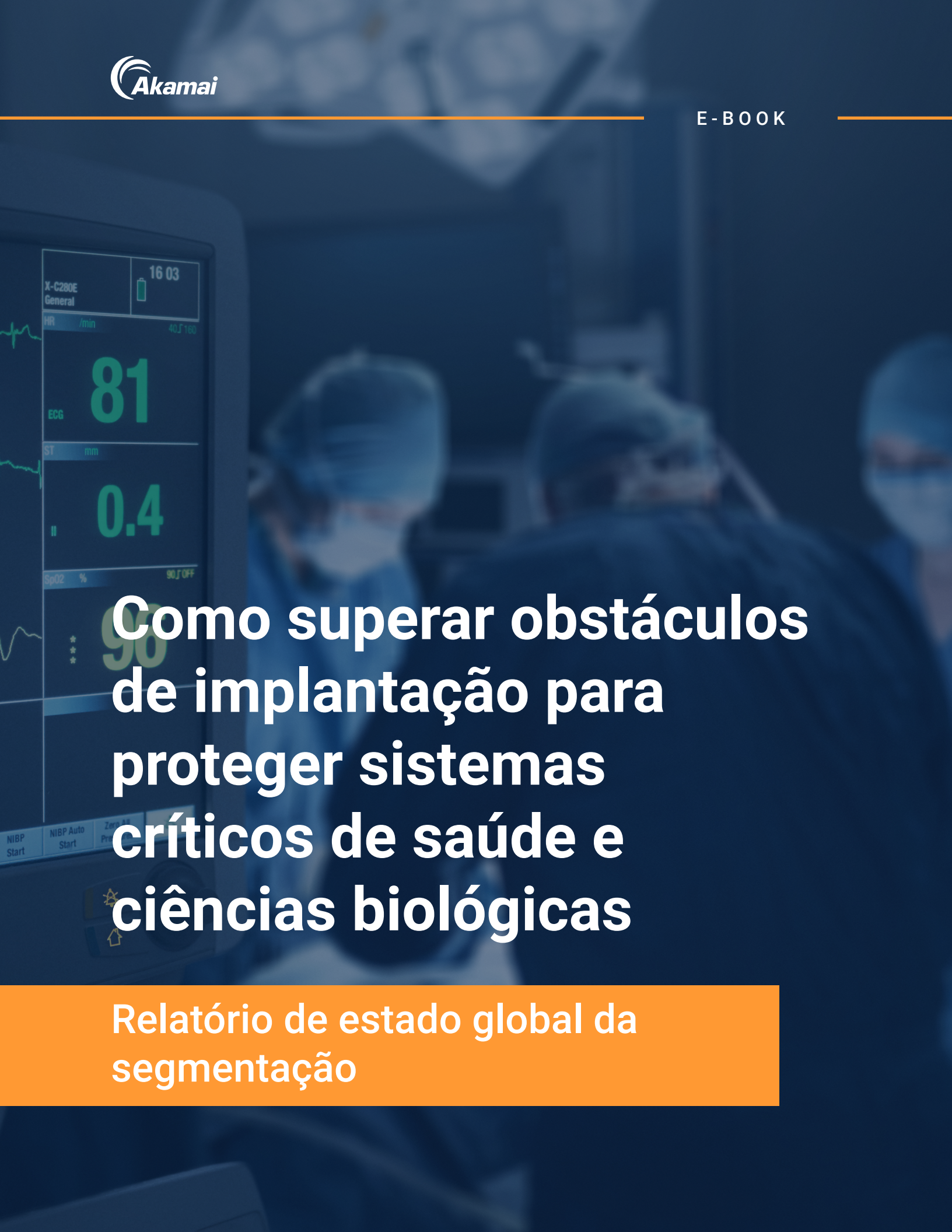
Akamai

E-BOOK



Como superar obstáculos de implantação para proteger sistemas críticos de saúde e ciências biológicas

Relatório de estado global da segmentação

Índice

Introdução

Agora, mais do que nunca, a TI da área de saúde afeta os dormitórios, a sala de reuniões e a sala de exames. As violações de dados de alto perfil estão aumentando em termos de gravidade e de frequência, com impactos operacionais e de reputação enormes. À medida que os agentes de ameaça usam táticas cada vez mais sofisticadas, e em muitos casos, unem forças, os perigos que o ecossistema de saúde enfrenta são mais frequentes e mais sérios. Devido a um grande volume de tecnologia herdadas, ao valor financeiro dos dados dos pacientes e aos desafios que envolvem a rápida digitalização e expansão da IoMT (Internet das Coisas Médicas), esse ambiente dinâmico precisa proteger sua infraestrutura, organização, aplicativos e APIs de maneiras inimagináveis há apenas cinco anos.

Como mostram as descobertas neste relatório, os ataques cibernéticos estão aumentando a pressão sobre os líderes de segurança para escolher as soluções corretas em um setor em que o funcionamento constante é uma questão de vida ou morte.

Os entrevistados das organizações de saúde e ciências biológicas nos Estados Unidos, América Latina, Europa, Oriente Médio, África e região Ásia-Pacífico concordam em grande parte sobre a eficácia da segmentação para manter os ativos protegidos. Mas os entrevistados também relatam que o progresso na implantação da segmentação em torno de aplicativos e ativos comerciais essenciais está abaixo do ideal. Os entrevistados (incluindo profissionais de saúde e especialistas em tecnologia de saúde, entre outras organizações especializadas em serviços ou produtos de saúde) afirmam que o principal obstáculo para as organizações de saúde e ciências biológicas tem sido a falta de conhecimento para implantar a segmentação. A complexidade histórica de implantar métodos tradicionais de segmentação, que não cobrem dispositivos médicos, é agravada pelo fato de que as equipes ainda estão sofrendo com as necessidades de pessoal que começaram antes da pandemia da COVID-19.

Uma pesquisa da HIMSS (Healthcare Information and Management Systems Society, Sociedade dos Sistemas de Informação e Gestão na Saúde), uma organização sem fins lucrativos dos EUA, constatou que 84% dos especialistas em TI nos EUA encontram dificuldade em atrair pessoal e 67% relatam que a permanência do pessoal é um problema. A HIMSS também constatou que a maioria dos funcionários não tem treinamento atualizado sobre ameaças predominantes e emergentes.

E no que consiste esse treinamento atualizado? 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, pacientes e reputação.

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 da 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 seus impactos

Os dados de 2021 em comparação com os de 2023 mostram que o número de ataques de ransomware (bem-sucedidos e malsucedidos) contra organizações de saúde em um período de 12 meses aumentou 162%. Os efeitos desses ataques podem variar desde o tempo de paralisação operacional, como procedimentos médicos cancelados ou remarcados, até problemas com interações de medicamentos devido à falta de acesso a registros médicos e desvios de ambulância para outras instalações de saúde.

Aumento percentual no número de ataques de ransomware nos últimos 12 meses por setor (dados de 2021 versus dados de 2023)

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 reflete o tamanho da base de 1.200 entrevistados, mostrando apenas o aumento percentual médio no número de ataques nos últimos 12 meses, dividido por setor.

Em média, a taxa de aumento para o setor de saúde é a mais alta entre todos os setores. Isso pode ser uma indicação de que as organizações de saúde, inclusive os hospitais infantis, que também são cada vez mais vítimas de ataques, têm menos probabilidade de serem vistas como “fora dos limites” pelos hackers.

Os ataques de ransomware contra organizações de saúde não apenas ocorreram com mais frequência em 2023 em comparação com 2021, mas também seus impactos foram mais prejudiciais (figura 2), com os entrevistados indicando aumentos nos danos à reputação, perda de fidelidade do cliente (paciente) e tempo de paralisação da rede. Todos esses fatores aumentam significativamente os desafios das equipes de segurança.

Essa pressão também afetou a criação de estratégias ágeis. O número de organizações de saúde que atualizam suas estratégias ou políticas de cibersegurança pelo menos uma vez por semana aumentou de 17% em 2021 para 25% em 2023, não apenas em resposta ao ransomware, mas também refletindo uma superfície de ataque em constante evolução.

Examinando isso mais profundamente, as organizações de saúde estão entre as que têm mais probabilidade de sofrer perda financeira após um ataque à cibersegurança em comparação com as de outros setores (43%, em comparação com 36% no geral). As organizações de saúde também têm maior probabilidade de sofrer perda de fidelidade do paciente/membro após um ataque à cibersegurança (48%, em comparação com 33% no geral). Isso mostra que, em muitos aspectos, as organizações de saúde correm maior risco do que outros tipos de organizações.

Impacto de ransomware/ataques cibernéticos na saúde e ciências biológicas

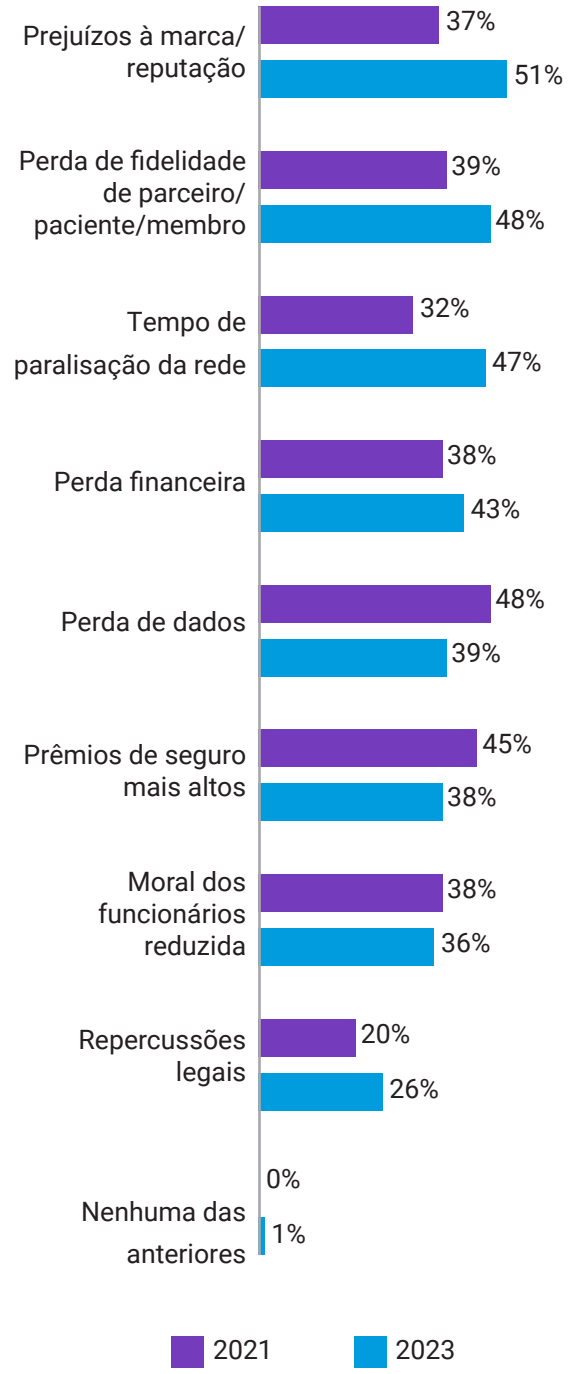


Fig. 2: quando sua organização detectou anteriormente ransomware ou algum outro ataque cibernético, quais dos seguintes impactos teve em sua organização? O gráfico mostra os tamanhos da base por ano, não mostrando todas as opções de resposta, divididos por dados históricos (2021 = 112, 2023 = 157), apenas dados do setor de saúde.

A segmentação aceita como pilar do Zero Trust

Os entrevistados no setor de saúde e ciências biológicas concordam que a segmentação é importante para garantir que suas organizações estejam seguras, principalmente no que se refere ao combate ao malware.

Zero Trust é uma estratégia de segurança de rede baseada na filosofia de que nenhuma pessoa ou dispositivo, dentro ou fora da rede de uma organização, deve receber acesso para se conectar aos sistemas ou cargas de trabalho de TI, a menos que seja explicitamente necessário. Em resumo, significa a ausência de qualquer confiança implícita.

64% por cento dos participantes da pesquisa afirmam que a segmentação é extremamente importante, e 94% acreditam que é fundamental impedir ataques prejudiciais.

A adoção do Zero Trust geralmente é motivada por circunstâncias além do controle dos líderes de TI na área da saúde. Ao citar por que sua organização começou um projeto de segmentação, um terço (33%) dos entrevistados da área de saúde diz que foi devido ao foco do governo na cibersegurança, e quase a mesma porcentagem (29%) diz que isso se deve a já terem sido vítimas de um ataque de ransomware.

Mas apenas cerca de um em cada três (34%) entrevistados da área de saúde relatam que sua estrutura Zero Trust está totalmente completa e definida e, portanto, consolidada. Esse percentual está entre os mais baixos em todos os setores, com alguns deles (como construção e serviços financeiros) sendo notavelmente mais propensos a ter uma estrutura Zero Trust consolidada em funcionamento (53% e 47%, respectivamente).

É provável que a consolidação do Zero Trust seja impulsionada por organizações de saúde nos EUA (onde 50% dizem que têm uma estrutura totalmente completa e definida), em comparação com outras regiões (apenas 23% de outros países e regiões dizem que sua estrutura Zero Trust está totalmente completa e definida).
Isso reflete a tendência geral, em que as organizações dos EUA em todos os setores relatam ser vítimas de ataques cibernéticos em comparação a outras regiões (115 nos últimos 12 meses, em comparação à média geral de 86).

As organizações de saúde, portanto, têm desafios quando se trata de Zero Trust. Os entrevistados desse setor têm maior probabilidade de ter encontrado problemas relacionados à tecnologia proprietária ao segmentar sua rede (41%, em comparação aos 32% no geral), e também têm maior probabilidade de enfrentar desafios orçamentários ao implementar o Zero Trust (47%, em comparação a uma média de 37% em todos os setores). O suporte de um parceiro experiente pode ajudar a superar alguns desafios: um dos aspectos mais difíceis de uma estrutura Zero Trust a ser implementada para organizações de saúde é a carga de trabalho de aplicativos (68%, em comparação com 60% no geral); um parceiro pode complementar as deficiências de qualificação, que foram relatadas por 45% das organizações de saúde.

A maioria dos entrevistados nas organizações de saúde deseja ir além e implementar a microssegmentação, que protege as cargas de trabalho dos aplicativos em um nível granular:

92% dos entrevistados do setor de saúde afirmam que a microssegmentação é, no mínimo, uma prioridade alta, sendo que 43% a consideram sua principal prioridade. Em todos os setores pesquisados, apenas 34% apresentam a microssegmentação como sua principal prioridade, demonstrando que as organizações do setor de saúde são mais propensas, em média, a valorizar e defender estruturas Zero Trust.

As implementações são lentas, mas a perseverança produz resultados transformadores

Mesmo com amplo reconhecimento de que a segmentação é essencial para evitar ataques cibernéticos, sua implantação é lenta.

Apenas 36% das organizações do setor de saúde segmentaram mais de duas áreas críticas de negócios em 2023, e 43% iniciaram um projeto de segmentação de rede há dois anos ou mais, o que sugere que os esforços foram interrompidos.

As áreas vitais da missão

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

As implementações lentas podem ser atribuídas a muitos dos principais obstáculos encontrados pelos entrevistados no setor de saúde: falta de qualificação/conhecimento para implementar a segmentação (45%), aumento dos gargalos de desempenho (como aqueles causados pela necessidade de solucionar erros manualmente, 44%) e o uso de tecnologia proprietária (41%, figura 3). A falta de qualificação/conhecimento especializado em particular é um problema para as organizações do setor da saúde, mais do que para as organizações de qualquer outro setor (todos inferiores aos 45% do setor da saúde, sendo a média vertical cruzada de 39%). Esses resultados se alinham com as descobertas recentes do Ponemon Institute, uma das principais organizações de pesquisa de segurança de TI, acerca das ameaças predominantes para o setor de saúde, que incluem principalmente ransomware e esquemas de comprometimento de e-mail comercial (BEC). Enquanto a remuneração competitiva para profissionais de TI da área da saúde é um desafio, o volume crescente de necessidades regulatórias complexas é outro.

Organizações de saúde em todo o mundo continuam a sentir os efeitos colaterais da pandemia da COVID-19 e da pressão que ela colocou sobre o capital humano e fiduciário, e isso compõe tais desafios.

Obstáculos encontrados durante a segmentação da rede nos setores de saúde e ciências biológicas

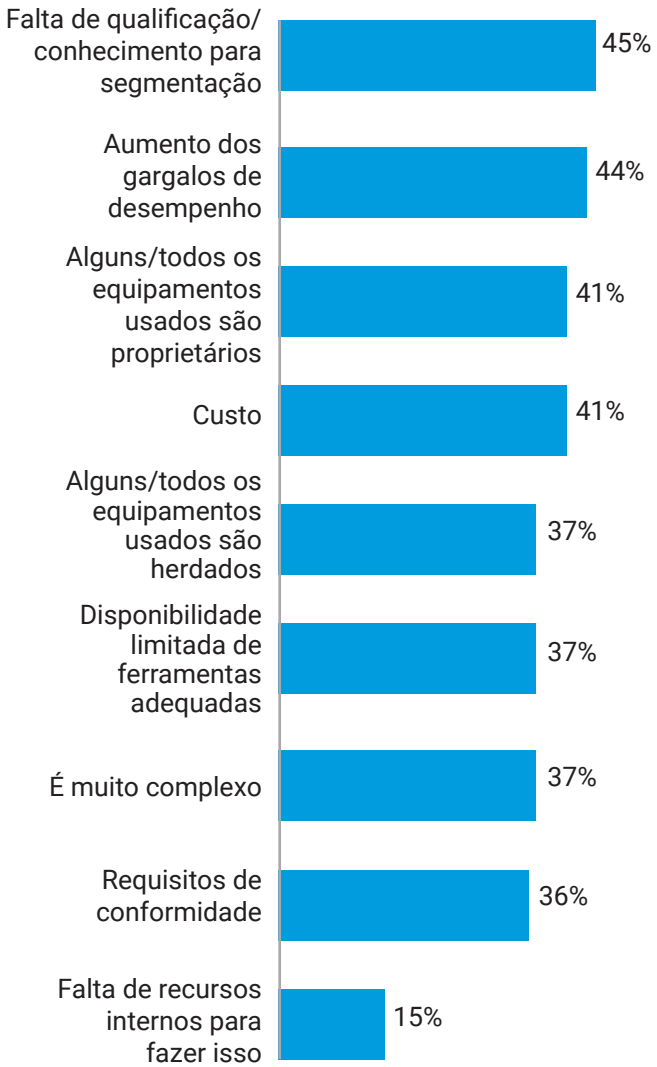


Fig. 3: quais problemas, se houver, sua organização encontrou/prevê ao segmentar a rede? O gráfico mostra o tamanho base de 2023 de 157, não mostrando todas as opções de resposta. Essa pergunta foi mostrada apenas aos entrevistados de organizações que segmentaram sua rede em algum momento, apenas dados do setor de saúde.

Apesar do progresso lento, as taxas de segmentação estão aumentando gradualmente em todos os setores. No setor da saúde, a porcentagem de organizações com segmentação de dados ou aplicativos críticos para os negócios aumentou 20% e os servidores segmentados aumentaram 18% de 2021 a 2023. Mas, embora esses aumentos ultrapassem os aumentos médios gerais observados em todos os setores (12% e 8%, respectivamente), as principais vulnerabilidades significam que as taxas de segmentação devem acelerar. É mais provável que, no setor de saúde, seja um funcionário/usuário de escritório o motivo de o invasor obter acesso à rede (47%, em comparação aos 26% no geral), e isso é mais do que o dobro de outros setores críticos para conformidade, como serviços financeiros e energia (ambos com 19%). O impacto desses ataques pode ser minimizado com a segmentação e, dada a importância de tantos sistemas dentro das organizações de saúde, com vidas em jogo, fica evidente o valor da implementação da segmentação o mais rápido possível.

Aprendizados da segmentação de seis áreas de negócios críticas

Aumentar a visibilidade reduz os riscos, o que é fundamental em um setor avesso a riscos. A proteção e a segmentação de mais ativos tornam as organizações de saúde mais seguras, permitindo que as equipes de segurança identifiquem mais rapidamente as ameaças e respondam com muito mais eficiência.

As descobertas da Vanson Bourne mostram que, após uma violação, a recuperação é 11 horas mais rápida com a segmentação. Os cálculos: para as organizações de saúde que implementaram a segmentação em seis áreas de missão crítica, são necessárias, em média, três horas para interromper completamente um ataque de ransomware; para aquelas com segmentação de apenas um ativo, esse tempo 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 aquelas com segmentação de 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 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 se tornou mais fácil de implementar.

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 novos segmentos ou de se preocupar com a localização física de 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 não depende do sistema operacional subjacente para a aplicação de políticas, ela funciona perfeitamente em computadores e sistemas operacionais: de servidores bare metal a implementações multinuvem, de tecnologia herdada como o Windows Server 2003 aos mais recentes sistemas de IoMT (Internet das Coisas Médicas) 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 em sua 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. O tempo e o esforço gastos para segmentar manualmente as áreas de negócios e, em seguida, solucionar manualmente problemas nessas áreas quando as coisas quebram podem ser enormes. 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 políticas e rótulos com tecnologia de IA e modelos de políticas 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 cliente, a Akamai entregou 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

Muitas organizações de saúde e ciências biológicas implantam o Akamai Guardicore Segmentation para garantir a conformidade com uma série de requisitos de conformidade nacionais e internacionais, como HIPAA, GDPR, PCI DSS e muitos outros. 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 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.

Conclusões

Os invasores cibernéticos estão visando as organizações do setor de saúde em um ritmo crescente: os ataques de ransomware contra organizações de saúde cresceram 162% de 2021 para 2023. Comparativamente, o setor de energia teve crescimento de 69% nesse período, e os serviços financeiros de 43%.

Provavelmente os entrevistados da área de saúde dirão que sua organização sofreu perdas financeiras após um ataque de cibersegurança: 43% relatam isso, em comparação aos 36% dos entrevistados em todos os setores.

A segmentação e a microssegmentação são mais importantes no setor de saúde do que em muitos outros setores: os responsáveis pelas decisões de segurança de TI em organizações de saúde (64%) têm maior probabilidade do que em muitos outros setores, como construção (58%), fabricação (53%) e comércio eletrônico (48%), de dizer que a segmentação de rede é extremamente importante para garantir que sua organização seja segura. As opiniões dos responsáveis pelas decisões de segurança de TI na área da saúde apresentam números muito próximos aos dos entrevistados em serviços financeiros e energia (ambos 66%).

É improvável que as organizações de saúde estejam mais consolidadas quando se trata de sua implantação de estrutura de segurança Zero Trust: é pouco provável que os profissionais do setor de saúde digam que a implantação do Zero Trust está completa e definida (34%), em oposição aos do setor de serviços financeiros (47%), do setor de energia (46%) e do setor de comércio eletrônico (42%).

Nosso grupo de pesquisa

Para o estudo de pesquisa completo, entrevistamos 1.200 responsáveis pelas decisões 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 participantes foram entrevistados em nível global, incluindo os Estados Unidos, Índia, México, Brasil, Reino Unido, França, Alemanha, China, Japão e Austrália. Eles eram de organizações com mais de mil funcionários de diversos setores e subverticais.

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.

Para os fins deste relatório de saúde e ciências da vida, analisamos 157 (2023) e 112 (2021) entrevistados que trabalham no setor. Esses entrevistados representam os mesmos países que o relatório principal (EUA, Índia, México, Brasil, Reino Unido, França, Alemanha, China, Japão e Austrália).

O estudo de pesquisa completo incluiu os seguintes setores adicionais: Comércio eletrônico (190), serviços financeiros (173), TI, tecnologia e telecomunicações (125), energia, petróleo/gás e serviços públicos (94), fabricação e produção (91), varejo, distribuição e transporte (81), mídia, lazer e entretenimento (63), construção e propriedade (60), serviços comerciais e profissionais (29), setor público (46), serviços ao consumidor (33), outros setores (58).

Saiba mais sobre a 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 saúde e ciências biológicas em akamai.com/healthcare e akamai.com/blog, ou siga a Akamai Technologies no X, antigo Twitter, e no 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, visite www.vansonbourne.com.