Akamai

E-BOOK

Como superar obstáculos de implantação para proteger sistemas de energia, petróleo e gás

Relatório sobre o estado global da segmentação

Índice

Introdução

Historicamente, os departamentos de segurança de TI e TO enfrentaram desafios significativos, mas no setor de energia, petróleo e gás e serviços públicos em geral, a pressão se torna ainda mais acentuada devido à natureza crítica dos serviços públicos em relação às populações. Conflitos regionais, pressões políticas e disputas ideológicas frequentemente agravam as dificuldades e aumentam os perigos enfrentados por esse setor. No entanto, à medida que os invasores se tornam mais sofisticados e combinam técnicas para apresentar ameaças maiores e mais frequentes, as equipes de segurança das organizações de energia sofrem uma pressão sem precedentes. Sem sistemas conectados online ou conectados a suas redes de TO privadas, é impossível que uma empresa de energia opere, e uma única violação bem-sucedida pode resultar em danos significativos à reputação e ao desempenho financeiro da organização.

As descobertas deste relatório indicam que as repercussões desses ataques estão se intensificando, aumentando assim a pressão sobre os executivos de segurança para selecionar as soluções apropriadas que garantam a segurança de todo o ambiente e preservam o desempenho.

Em contraste, órgãos reguladores e governos de todo o mundo estão atualmente formulando diretrizes e regulamentos de segurança em resposta ao aumento substancial das ameaças à cibersegurança encontradas por esse setor e à natureza crítica dos serviços que ele fornece. As empresas de energia são obrigadas a aderir aos padrões regulatórios e garantir a manutenção e a segurança dos serviços.

Os entrevistados nas organizações do setor de energia (representando todas as regiões, incluindo EUA, América Latina, EMEA e APAC) concordam com a eficácia da segmentação para manter os ativos protegidos, mas o progresso geral na implantação dessa segmentação em torno de aplicativos e ativos comerciais críticos é menor do que o esperado. O principal obstáculo para as organizações de energia tem sido o aumento dos gargalos de desempenho, o que sugere que as equipes podem hesitar em embarcar em um projeto que poderia interromper o desempenho, sem garantias de que isso não vai acontecer. É fundamental ter em mente que, dada a natureza vital dos serviços prestados ao público por essas organizações, as interrupções na funcionalidade das soluções podem resultar em danos aos clientes ou comprometer a segurança da equipe de manutenção.

Por outro lado, espera-se que o setor de energia dê maior ênfase à segmentação do que a maioria dos outros setores, indicando que seu valor é, sem dúvida, reconhecido.

No geral, a segmentação progrediu com lentidão, mas aqueles que persistiram 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. Essa abordagem granular à segurança permite um controle mais preciso sobre o acesso e a proteção de dados confidenciais. Ao implementar a microssegmentação, as organizações podem limitar o impacto de uma violação de segurança e proteger melhor sua rede contra ciberameaças avançadas. Em geral, a combinação de segmentação e microssegmentação fornece uma estratégia de segurança abrangente que é essencial para proteger ativos críticos no atual cenário de ameaças complexo e dinâmico.

Os ataques de ransomware continuam aumentando, assim como o impacto deles

O número de ataques de ransomware (bem-sucedidos e malsucedidos) em organizações de energia aumentou significativamente nos últimos dois anos, de 37 em média em 2021 para 62 em 2023, e não há motivo para suspeitar que esse crescimento não continuará a curto prazo. Os impactos podem ter efeitos prejudiciais sobre a população e as economias, incluindo quedas de energia ou danos à infraestrutura, levando à perda de credibilidade da empresa, roubo de informações pessoais e comerciais, ou até mesmo risco para a vida das pessoas. Com o aumento da frequência e da gravidade dos ataques de ransomware, é fundamental que as organizações de energia protejam seus dados e sistemas. Não fazer isso não só coloca a organização em risco, mas também prejudica a integridade e a segurança de indivíduos e comunidades que dependem desses serviços. À medida que os ataques de ransomware se tornam mais sofisticados, é fundamental que as organizações permaneçam vigilantes e proativas em suas estratégias de defesa para mitigar possíveis danos e interrupções causados por essas ameaças mal-intencionadas.

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

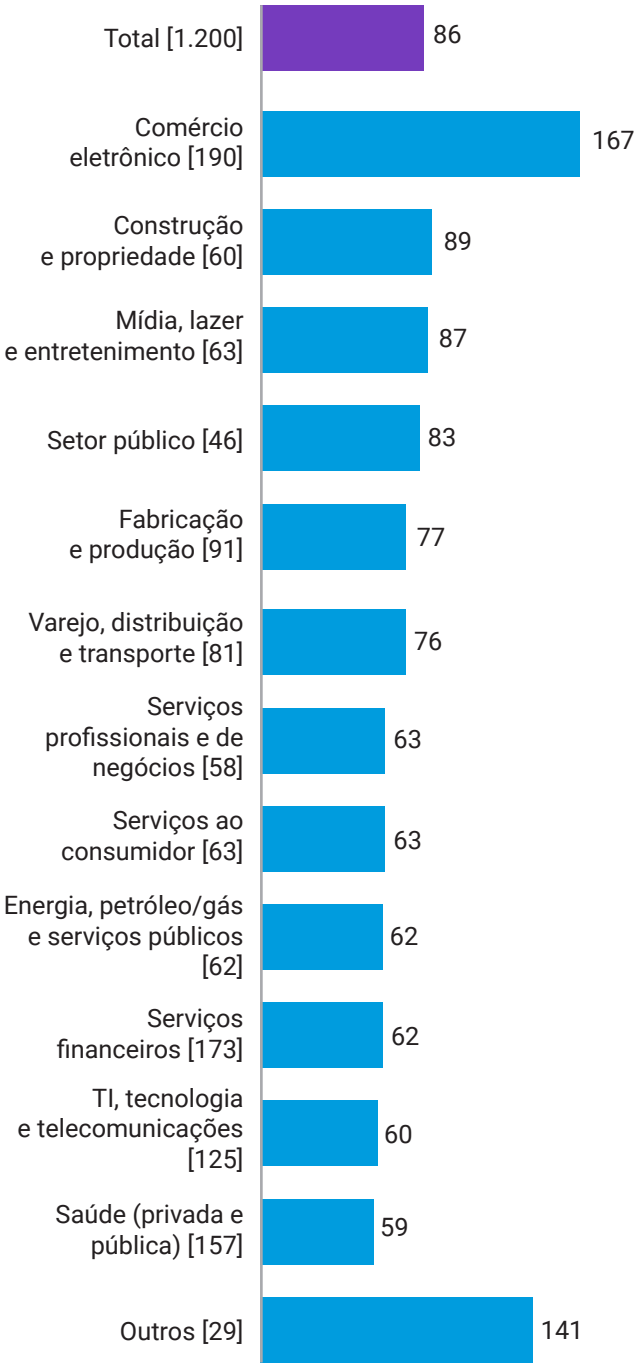

Fig. 1: quantos ataques de ransomware foram feitos contra sua organização nos últimos 12 meses (independentemente de terem sido bem-sucedidos ou não)? O gráfico mostra o número médio de ataques nos últimos 12 meses, números base divididos por setor.

Uma razão para esse número relativamente baixo de ataques é que o principal ativo de uma empresa de energia tende a ser físico (petróleo, gás etc.) em vez de digital (dinheiro ou dados do cliente). Elas também não são conhecidas por serem alvos "fracos/fáceis", como algumas outras organizações com relativamente poucas regulamentações em vigor, como mídia ou varejo. Isso significa que os ataques podem ser mais suscetíveis de serem motivados por objetivos políticos do que por objetivos financeiros. Essa afirmação é potencialmente sustentada pelo fato de que, embora apenas 5% dos entrevistados em todos os setores em geral tenham dito que sua organização nunca detectou um ataque cibernético, esse número aumenta para 24% dos entrevistados no setor de energia.

Os ataques de ransomware no setor de energia foram mais frequentes em 2023 do que 2021, mas a gravidade do impacto conta uma história mais complexa (figura 2), com nossos entrevistados indicando um aumento considerável na perda de dados, mas reduções em todos os outros problemas. Essa grande tendência pode ser impulsionada pelo aumento da conscientização do valor dos dados (que são priorizados como alvo por hackers), mas também pode ser devido a melhorias na abordagem no setor de energia. O número de organizações de energia que estão atualizando estratégias ou políticas de cibersegurança pelo menos uma vez por semana aumentou de apenas 2% em 2021 para 23% em 2023. Com eventos globais (principalmente relacionados a conflitos ou mudanças climáticas) fazendo com que os países prestem mais atenção à sua segurança de energia, não é nenhuma surpresa ver as organizações de energia aumentando o foco em estratégias de cibersegurança.

Impacto de ransomware/ataques cibernéticos no setor de energia

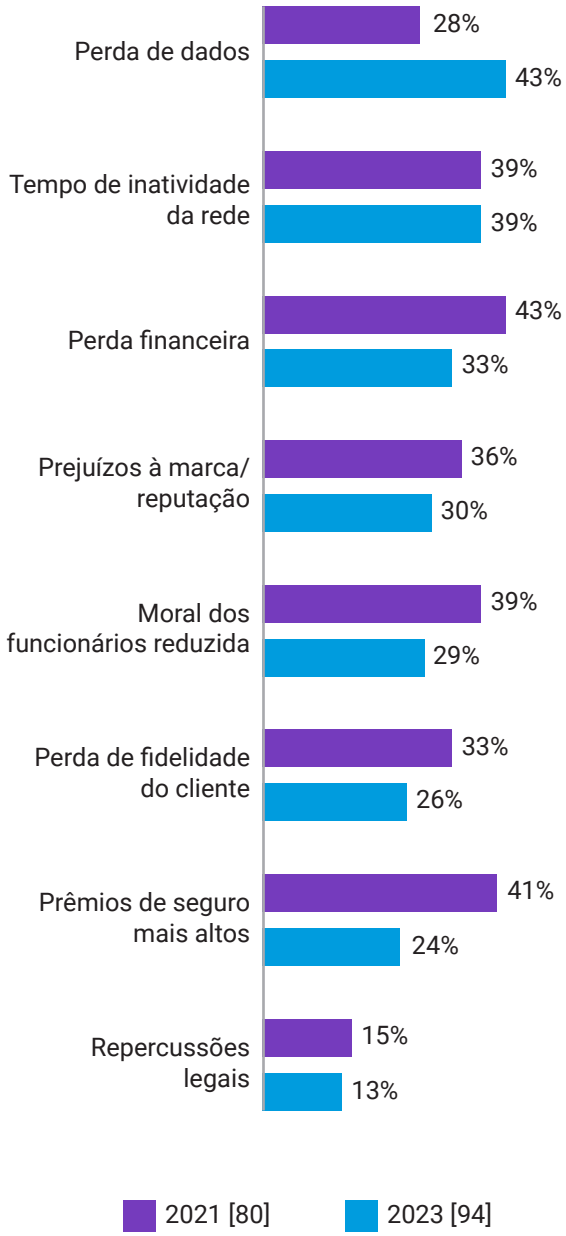

Fig. 2: quando sua organização detectou anteriormente ransomware ou algum outro ataque cibernético, qual dos seguintes impactos sua organização sofreu? O gráfico mostra os tamanhos da base por ano (não mostrando todas as opções de resposta) divididos por dados históricos. Dados apenas do setor de energia.

A segmentação é amplamente reconhecida como parte importante do Zero Trust

Nossos entrevistados do setor de energia concordam que a segmentação é importante para garantir a segurança de suas organizações, principalmente no que se refere ao combate ao malware. Dos entrevistados, 66% (entre os maiores de todos os setores) afirmam que ela é extremamente importante, e 95% acreditam que ela é fundamental para ajudar a impedir ataques prejudiciais.

A segmentação também contribui significativamente para uma estrutura Zero Trust, e a boa notícia para as organizações de energia é que já foram feitos progressos nessa área. Todas (100%) estão implantando ou já implantaram uma estrutura de segurança Zero Trust, embora menos da metade (46%) declare que sua estrutura Zero Trust está totalmente completa e definida e, portanto, madura. Portanto, essa é uma área em que a segmentação pode ajudar as organizações de energia em sua jornada rumo ao Zero Trust. Esse é o resultado da pesquisa sobre os ambientes de TI das organizações, embora o ambiente de TO possa ser diferente devido às tecnologias utilizadas.

A maioria dos entrevistados nas organizações de energia deseja ir além e implementar a microssegmentação, que protege as cargas de trabalho dos aplicativos em um nível granular: dentre eles, 88% afirmam que a microssegmentação é, no mínimo, uma alta prioridade, sendo que 47% a consideram sua principal prioridade. Em todos os setores, apenas 34% apresentam a microssegmentação como prioridade principal, demonstrando que as organizações do setor de energia são, em média, mais propensas a realizarem essa implementação o mais rápido possível. Além disso, quase todos (98%) os tomadores de decisão de TI e segurança no setor relatam que a microssegmentação foi adotada por pelo menos uma minoria do setor, enfatizando que é uma solução de amplo reconhecimento.

As implementações são lentas, mas a perseverança produz resultados transformadores

A dura realidade: mesmo com um consenso tão amplo de que a segmentação é a chave para impedir os ataques, a implantação da segmentação tem sido mais lenta do que o esperado. Apenas 38% das instituições do setor de energia segmentaram mais de duas áreas críticas de negócios em 2023 (em comparação com 30% em 2021), e 33% iniciaram pela primeira vez um projeto de segmentação de rede há dois ou mais anos, o que sugere que os esforços ficaram parados.

As implantações lentas são explicadas com mais clareza pelos principais obstáculos encontrados pelos entrevistados: aumento dos gargalos de desempenho (49%), requisitos de conformidade (43%) e equipamentos proprietários (41%, figura 3).

Obstáculos encontrados durante a segmentação da rede no setor de energia

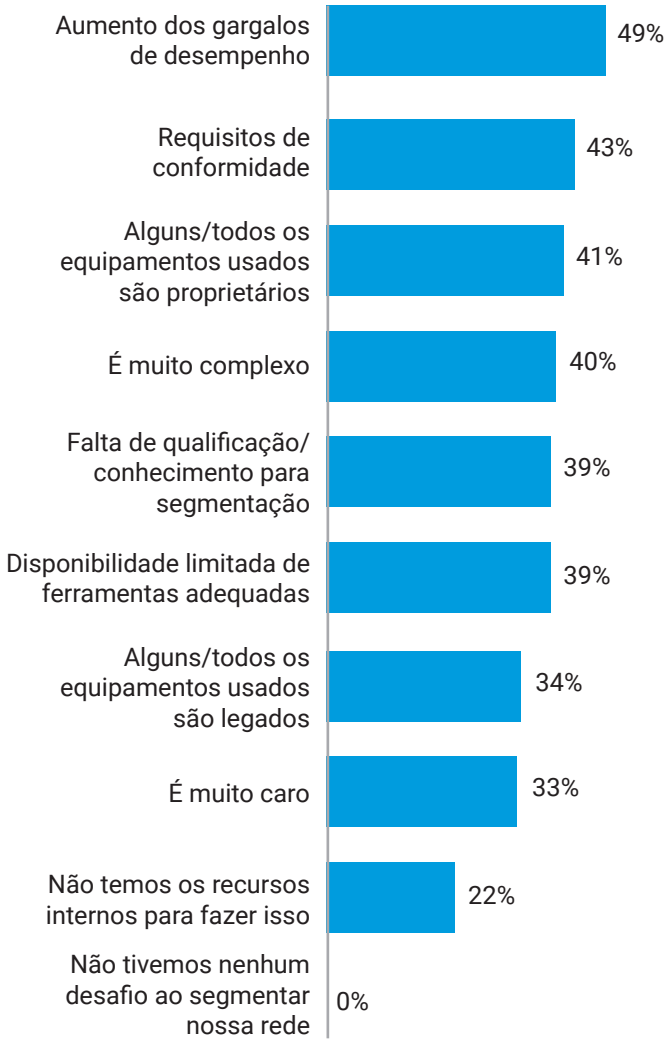

Fig. 3: quais problemas, se houver, sua organização encontrou/ prevê ao segmentar a rede? O gráfico mostra o tamanho da base de 94. Pergunta mostrada apenas para aqueles que segmentaram sua rede em algum momento, não mostrando todas as opções de resposta. Dados apenas do setor de energia.

Um fato encorajador para o setor de energia, no entanto, é que 42% relatam que seu projeto de segmentação de rede começou como resultado de uma recomendação da liderança/conselho administrativo. Esse é o mais elevado de todos os setores (a média geral é de 28%) e demonstra que a segmentação é claramente reconhecida como importante no setor.

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 sugere que você está apenas gerenciando uma solução com uma única interface para visualizar e gerenciar as conexões feitas por vários sistemas operacionais e dispositivos em todo seu ambiente, independentemente da localização física.

É importante observar que a solução Akamai Guardicore Segmentation também pode ser usada em ambientes de TO, permitindo que a microssegmentação seja aplicada a redes de controle privadas, sistemas operacionais legados e dispositivos de Internet das coisas sem agentes.

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 acompanham você durante todo o processo de implantação para garantir que suas metas de segmentação em seu ambiente exclusivo de TI ou TO 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 implantam nossa solução para garantir e atestar a conformidade com várias exigências de conformidade domésticas e internacionais, como PCI DSS, SWIFT, Sarbanes-Oxley, HIPAA, GDPR, LGPD 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. No caso de uma violação, os esforços de recuperação são seguros e levam menos tempo para serem concluídos, já que o impacto deve ser limitado apenas ao segmento afetado.

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

A segmentação e a microssegmentação são mais importantes no setor de energia do que em muitos outros setores: os tomadores de decisão de TI, TO e segurança de TI de organizações do setor de energia (66%) são mais propensos a dizer que a segmentação de rede é extremamente importante para garantir que a organização esteja segura do que aqueles do setor de serviços ao consumidor (36%), mas menos provável do que aqueles de TI e tecnologia (73%).

Empresas do setor de energia são muito mais propensas a dizer que a microssegmentação é a maior prioridade (47%) do que as do setor de serviços ao consumidor (12%), e apenas um pouco menos propensas do que as do setor público (48%).

Empresas do setor da energia estão entre as menos prováveis de não terem feito nenhuma segmentação: é improvável que os entrevistados de organizações do setor de energia digam que nenhum ativo crítico para os negócios tenha sido segmentado (4%), embora ainda seja mais provável do que os dos setores de construção, de serviços ao consumidor e de mídia (todos 0%), mas menos provável do que os do setor público (15%).

Empresas do setor de energia estão entre as mais prováveis de terem feito o maior progresso com a segmentação: as organizações do setor de energia são apenas um pouco menos propensas a terem segmentado mais de dois ativos críticos para os negócios (38%) do que aquelas do setor varejista (43%) e muito mais do que aquelas do setor de serviços ao consumidor (3%).

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 EUA, Índia, México, Brasil, Reino Unido, França, Alemanha, China, Japão e Austrália. Elas faziam parte 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.

Para os fins deste relatório, analisamos 94 (2023) e 80 (2021) entrevistados que trabalham no setor de energia.

Saiba mais sobre o 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 tudo o que for possível. Saiba mais sobre as soluções da Akamai em akamai.com 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 mais informações, visite www.vansonbourne.com.