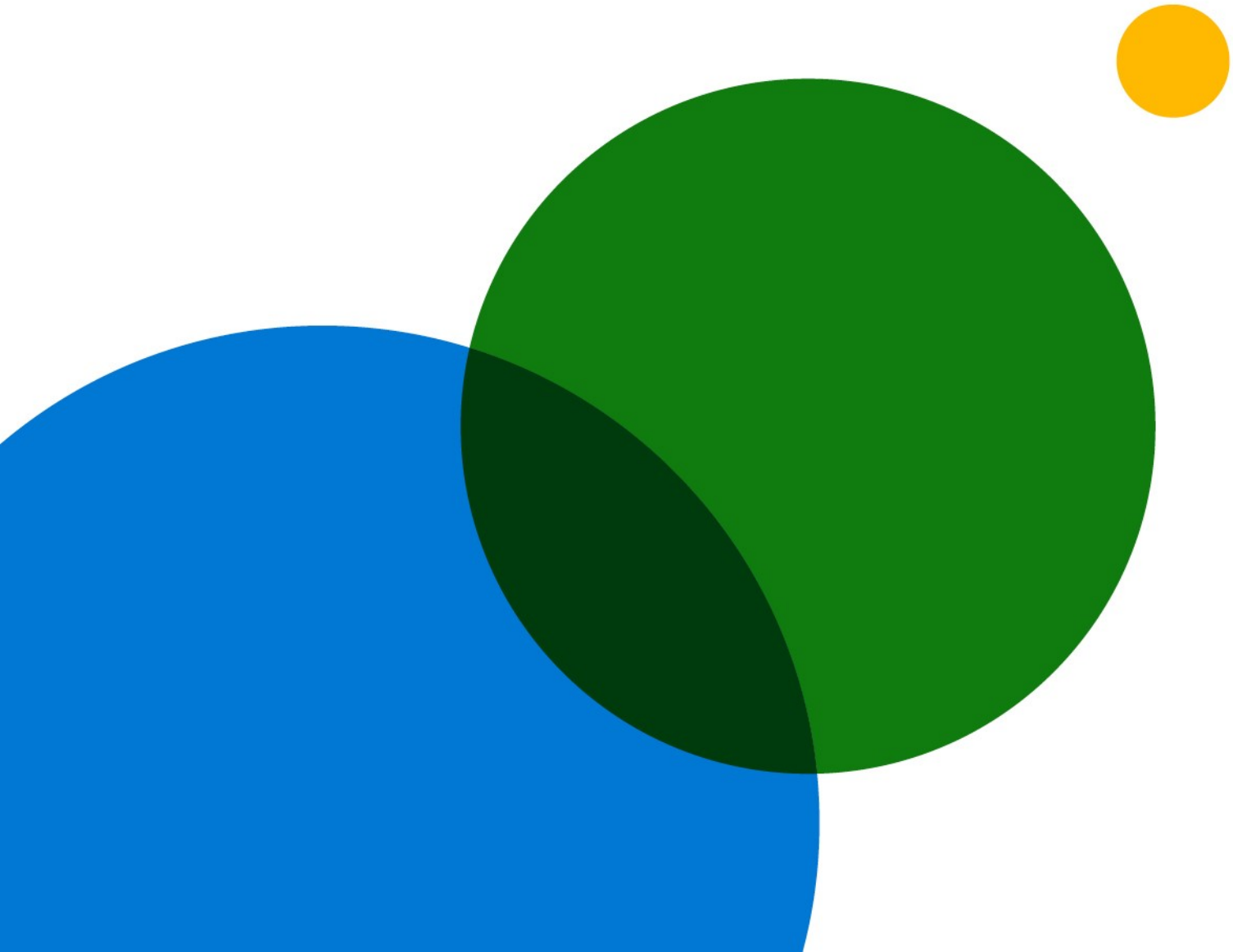
Microsoft Security

hypothesis

Relatório de adoção de confiança zero



Sumário

Introdução

Vasu Jakkal/vice-presidente corporativo de segurança, conformidade e identidade

No ano passado, foi notável a evolução da segurança cibernética e a ascensão da confiança zero como uma estratégia orientadora para nossa indústria e organizações de todo o mundo.

No início da pandemia, o local de trabalho tornou-se quase totalmente remoto da noite para o dia. Essa mudança forçou muitas organizações a se adaptarem rapidamente para dar suporte aos funcionários que estavam desempenhando suas tarefas como podiam, usando dispositivos pessoais, colaborando por meio de serviços de nuvem e compartilhando dados fora do perímetro da rede corporativa. À medida que as organizações se adaptavam a essa transformação, elas também enfrentaram criminosos cibernéticos cada vez mais sofisticados que evoluem continuamente sua segmentação, táticas e recursos.

Hoje, o trabalho híbrido é a nova realidade. Neste cenário e diante da mudança rápida, as organizações que pesquisamos nos disseram que dependem de confiança zero para aumentar a agilidade de segurança e conformidade, aumentar a velocidade de detecção e correção de ameaças e aumentar a simplicidade e a disponibilidade da análise de segurança.

Com base nos princípios da verificação explícita, uso de acesso menos privilegiado e presunção de violação, uma arquitetura abrangente de confiança zero cria proteções dentro e entre identidades, pontos de extremidade, aplicativos, infraestrutura, rede e dados, em parceria com maior visibilidade, automação e orquestração. Nós recomendamos essa abordagem com nossos clientes e parceiros e a adotamos em nossa abordagem de segurança global e desenvolvimento de software aqui na Microsoft.

Este relatório facilita a adoção da confiança zero em diversos mercados e indústrias. Esperamos que a aprendizagem adquirida por meio desta pesquisa possa ajudar a acelerar a sua própria adoção da estratégia de confiança zero, ajuda a esclarecer o progresso coletivo de seus colegas e fornecer insights sobre o estado futuro desse espaço em rápida evolução.

Metodologia

A Microsoft encarregou o Hypothesis Group, uma agência de insights, design e estratégia, de realizar a pesquisa e o Relatório de adoção de confiança zero. A pesquisa incluiu duas fases nos EUA para destacar tendências e o momento na adoção da confiança zero, com mercados adicionais incluídos na segunda fase para descobrir as tendências globais.

Pesquisas iniciais ocorreram em agosto de 2020, quando uma pesquisa online de 15 minutos foi realizada nos EUA com 300 tomadores de decisões de segurança (SDMs) envolvidos em decisões de estratégia de confiança zero em empresas de diversas indústrias. Além da pesquisa online, cinco entrevistas detalhadas foram realizadas online em setembro de 2020 entre os SDMs dos EUA de diversas indústrias.

Em abril de 2021, a pesquisa global foi realizada nos EUA, Alemanha, Japão e Austrália/Nova Zelândia em um grupo semelhante de tomadores de decisões de segurança. Mais de 900 participantes fizeram uma pesquisa online de 15 minutos com perguntas sobre sua adoção de estratégia de confiança zero, práticas recomendadas, benefícios, desafios e como pretendem investir no futuro.

Observações importantes sobre a adoção da confiança zero

01/ As organizações estão prontas para tirar proveito da estratégia de confiança zero, acelerada pela migração para um local de trabalho híbrido e a Covid-19

Os tomadores de decisões de segurança (SDMs) dizem que o desenvolvimento de uma estratégia de confiança zero é sua prioridade de segurança, e 96% afirmam que ele é fundamental para o sucesso de sua organização. Os principais motivadores para adotar uma estratégia de confiança zero são melhorar sua postura geral de segurança e a experiência do usuário final. A mudança para um local de trabalho híbrido, acelerada pelo COVID-19, também está impulsionando a adoção mais ampla da estratégia de confiança zero: 81% das organizações empresariais iniciaram a migração para um local de trabalho híbrido, e 31% já concluíram o processo. No entanto, 94% têm preocupações sobre a transição, principalmente, o uso indevido de funcionários, aumento de workloads da TI e ciberataques. Diante disso, as principais considerações para uma estratégia incluem o aumento do treinamento para funcionários e a autenticação multifatorial (MFA) para garantir uma experiência de usuário e uma transição tranquilas.

02/ A estratégia de confiança zero permite flexibilidade. Assim, as organizações podem começar a implementar para que a abordagem possa ser adaptada às suas necessidades

Menos de 15% das organizações começaram a implementar a estratégia de confiança zero na mesma área de risco de segurança. Isso ocorre em grande parte porque a implementação é abordada como um processo de ponta a ponta entre pilares e recursos da arquitetura de segurança, e não como uma série de tecnologias individuais diferentes. Da mesma forma, a ordem na qual os componentes individuais da confiança zero dentro de uma área de risco de segurança são implementadas é altamente variável, e os profissionais de segurança diferem substancialmente em quais componentes eles começam a implementar primeiro.

03/ Embora a estratégia de confiança zero seja amplamente adotada e melhore a capacidade das organizações de gerenciar ameaças, ainda há trabalho a ser feito

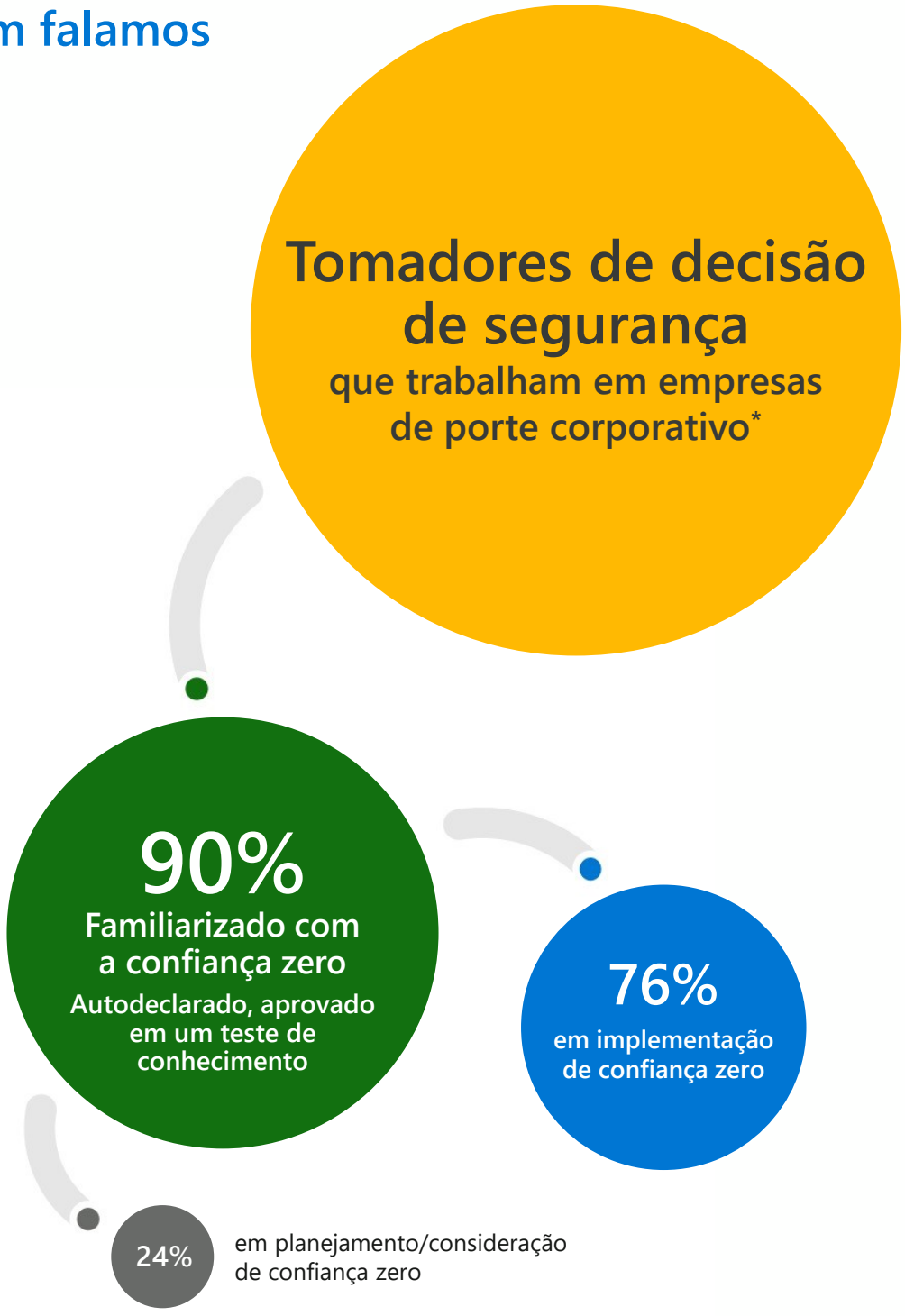
76% das organizações pelo menos começaram a implementar uma estratégia de confiança zero, e 35% afirmam que foram totalmente implementadas. No entanto, aqueles que alegam ser totalmente implementados admitem que não concluíram a implementação da estratégia de confiança zero em todas as áreas e componentes de risco de segurança. A estratégia de confiança zero é atraente porque fornece maior agilidade, velocidade de detecção de ameaças e melhor capacidade de gerenciar a segurança da Internet das Coisas (IoT) e da tecnologia operacional (OT). A adoção está crescendo nos EUA (70% em agosto de 2020 a 79% em abril de 2021); os EUA também estão mais à frente na implementação de confiança zero em relação a outros países que começaram a adotar posteriormente, e as organizações nos EUA afirmam ser menos limitadas pelos orçamentos. No entanto, embora 57% das organizações afirmem estar à frente dos outros quando se trata de adoção, cerca de metade ainda tem mais trabalho a fazer, pois não implementou totalmente a confiança zero em todas as áreas e componentes de risco de segurança.

04/ Olhando para o futuro, a estratégia de confiança zero permanecerá uma prioridade máxima e exigirá uma tomada de decisão cuidadosa quando se trata de funcionários e fornecedores

Espera-se que a estratégia de confiança zero continue sendo a prioridade de segurança daqui a dois anos, e as organizações antecipam aumentar seu investimento. Superar os desafios com seus funcionários (incluindo equipes de segurança de pessoal e adesão da liderança) será fundamental para duplicar o investimento de confiança zero. Quando se trata de estratégia de fornecedores, os tomadores de decisão de segurança têm uma ligeira preferência por trabalhar com provedores holísticos ou consolidados, já que a seleção de fornecedores é muitas vezes contingente à disponibilidade de experiência interna. Os benefícios da melhor abordagem incluem maior especialização, recursos e simplicidade, embora a implementação possa levar mais tempo, ser mais difícil de integrar na arquitetura de segurança existente e aumentar a vulnerabilidade potencial.

Com quem falamos

Global



*mais de 1.000 funcionários nos EUA; mais de 500 funcionários na Alemanha, Japão, Austrália/Nova Zelândia

Aprendizados gerais de pesquisa

As organizações estão prontas para tirar proveito da estratégia de confiança zero

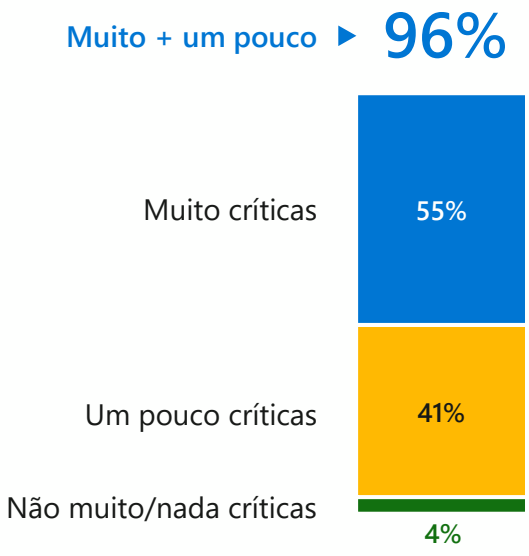
A estratégia de confiança zero é a prioridade de segurança de hoje em mercados e indústrias, com várias organizações adotando uma estratégia de confiança zero nos últimos anos. Embora a confiança zero seja prioridade para todos (53%), ela é uma prioridade particularmente alta para as organizações nos Estados Unidos (56%) e na Alemanha (53%).

Quase todos os profissionais de segurança (96%) acreditam que uma estratégia de confiança zero é fundamental para o sucesso de sua organização. (Consulte a Exibição 1) Além de fortalecer sua postura geral de segurança e melhorar a experiência do usuário final, os profissionais de segurança estão buscando uma estratégia de confiança zero para simplificar os procedimentos de segurança para os funcionários. (Consulte a Exibição 2)

Como explica um tomador de decisões de segurança do setor de hotelaria dos EUA, "*O objetivo é melhorar a nossa postura de segurança em geral, mas é tudo uma questão de reduzir o atrito na experiência do usuário final e tornar a vida mais fácil para ele.*"

Além disso, 31% dos profissionais de segurança veem a estratégia de confiança zero como uma ferramenta importante na mudança iminente para um local de trabalho híbrido pós-pandemia. Esse impulsionador é particularmente saliente na Austrália/Nova Zelândia (44%).

Exibição 1. A confiança zero é fundamental



Exibição 2. Motivadores da confiança zero

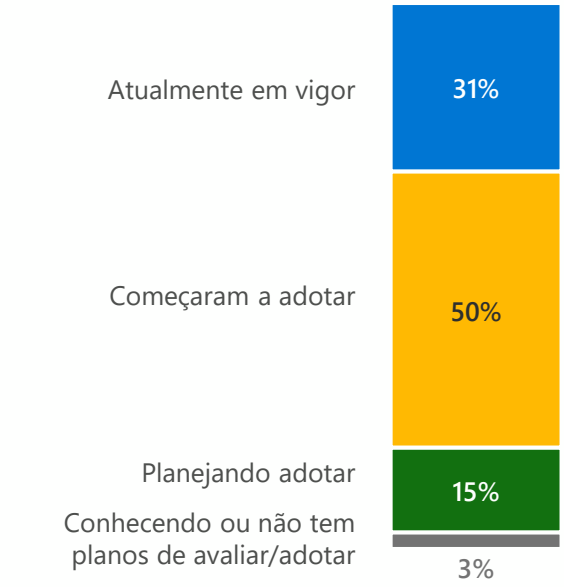
Principais motivadores	
Melhore sua postura geral de segurança	47%
Melhore a experiência e a produtividade do usuário final	44%
Transforme a maneira como as equipes de segurança trabalham juntas	38%
Simplifique a camada de segurança	35%
Reduza os custos da segurança	35%

A mudança para um local de trabalho híbrido está impulsionando uma adoção mais ampla da estratégia de confiança zero

81% das organizações iniciaram a migração para um local de trabalho híbrido, e 31% já concluíram o processo. Dito isso, as taxas de adoção total são inconsistentes entre os mercados: enquanto a Austrália e a Nova Zelândia lideram com 37%, a Alemanha está muito atrás, com apenas 20% das organizações já migradas para um modelo híbrido. (Consulte a Exibição 3)

Mesmo à medida que os mercados globais avançam em direção a um local de trabalho híbrido com taxas diferentes, a grande maioria (91%) das organizações que não concluíram a transição preveem que isso ocorrerá nos próximos cinco anos. Crucialmente, 94% estão preocupados com a transição, e as principais preocupações são com o uso indevido de funcionários e o aumento dos workloads da TI e do risco de ciberataques. (Consulte a Exibição 4)

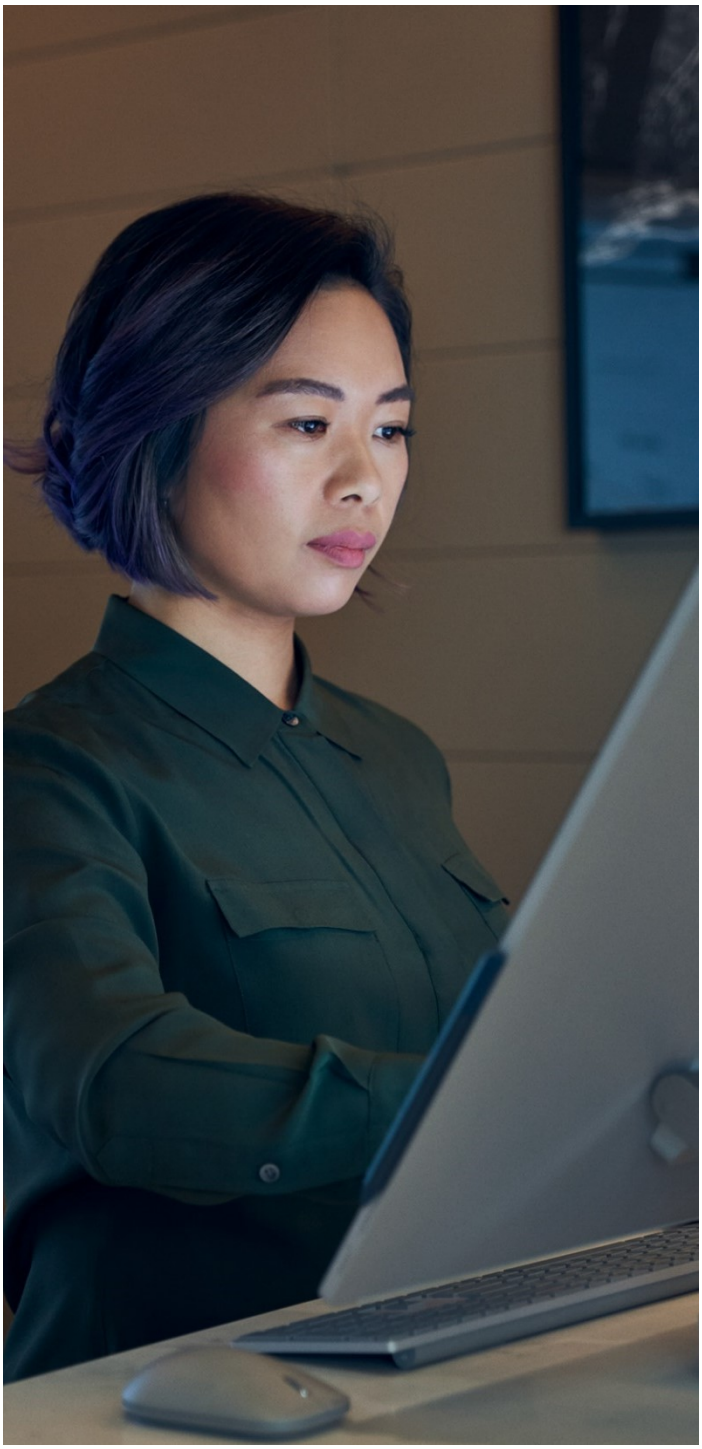
Exposição 3. Intenção de local de trabalho híbrido



Exposição 4. Preocupações com o local de trabalho híbrido

Funcionários que fazem download de aplicativos inseguros	37%
Aumento do workload de TI	37%
Ataque de ransomware	36%
Ataques de phishing	35%
Uso indevido de dispositivos pessoais	34%
Acesso não autorizado aos dados	31%
Incapacidade de gerenciar todos os dispositivos	30%
Uso de contas de email pessoais	30%
Não conformidade com os regulamentos de dados	24%

A Covid-19 trouxe novas considerações que aceleram a migração para a estratégia de confiança zero



Em um esforço para minimizar possíveis problemas, os stakeholders enfatizam a importância de mais treinamentos para os funcionários (54%) (particularmente no Japão (61%) e na Alemanha (58%)) e da autenticação multifatorial (MFA) (50%) (particularmente nos Estados Unidos (52%) e na Alemanha (56%)) para garantir uma experiência de usuário e uma transição tranquilas.

Como o trabalho seguro remoto e híbrido pode ser auxiliado pela estratégia de confiança zero, a COVID-19 acelerou a adoção de uma estratégia de confiança zero para 72% das organizações, embora as assimetrias surjam entre os mercados. Enquanto a pandemia catalisou a adoção de cerca de sete em cada dez organizações nos EUA (76%), Japão (71%) e Austrália/Nova Zelândia (69%), as taxas de implementação foram notavelmente menores na Alemanha (62%), talvez devido a uma transição mais lenta para um local de trabalho híbrido.

A confiança zero é amplamente implementada em todo o mundo e cresce nos EUA

A confiança zero não é apenas um chavão; é uma realidade. Pelo menos 76% das organizações começaram a implementar essa estratégia, e 35% acreditam que estão totalmente implementadas. No entanto, esses dados dão uma ideia excessivamente otimista, pois muitas organizações que se consideram totalmente implementadas não concluíram a execução em todas as áreas de risco de segurança. Hoje, os EUA estão à frente na adoção da estratégia de confiança zero em relação a outros mercados e continuam a crescer rapidamente: em comparação com agosto de 2020, a implementação de estratégia de confiança zero nos EUA aumentou de 70% para 79%, um salto considerável em apenas oito meses. (Consulte a Exibição 5)

Embora a estratégia de confiança zero atualmente predomine o espaço de segurança, sua onipresença é relativamente nova. 82% das empresas implementaram estratégias de confiança zero nos últimos três anos, com 21% fazendo isso nos últimos 12 meses. Dito isso, 26% das organizações dos EUA iniciaram a implementação há mais de 3 anos, contra 19% das organizações japonesas, 6% das organizações na Austrália/Nova Zelândia e 3% das organizações na Alemanha. Essa implementação anterior nos EUA — em conjunto com menos restrições orçamentárias — pode ajudar a explicar por que as organizações nos EUA estão à frente na adoção da confiança zero em comparação com as organizações em outros mercados. De modo semelhante, o surgimento relativo da confiança zero na Alemanha ajuda a contextualizar suas menores taxas de adoção: 97% das organizações alemãs só começaram a implementação nos últimos três anos.

Exibição 5. Implementação da confiança zero

	EUA (2020)	EUA	DE	JP	AUS/NZ
Implementação da confiança zero	70%	79%	75%	76%	71%
• Totalmente implementadas	27%	44%	19%	32%	28%
• Em andamento	43%	35%	56%	44%	43%

35% totalmente implementadas

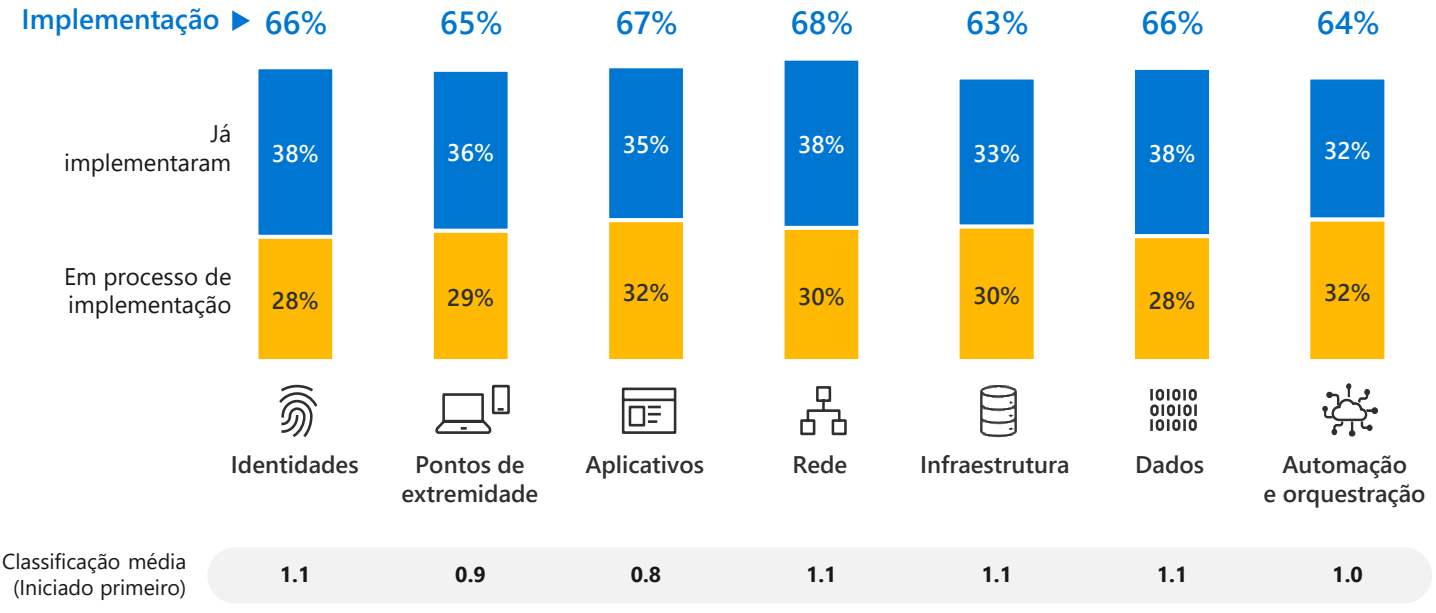
42% de progresso na implementação

Não há uma abordagem única para a implementação de confiança zero, dando permissão para começar em qualquer lugar

Nenhuma área de risco de segurança única (identidades, pontos de extremidade, aplicativos, rede, infraestrutura, dados, automação e orquestração) se destaca como um ponto de partida primário para a estratégia de confiança zero, pois menos de 15% começam com a mesma área de risco de segurança. As organizações estão começando em lugares diferentes, provavelmente com base em suas necessidades e recursos internos disponíveis. Por fim, eles buscam adotar uma estratégia de confiança zero em todas as áreas de risco de segurança para garantir ainda mais proteção contra ameaças, de modo que a confiança zero é percebida como uma estratégia de ponta a ponta a ser concluída ao longo do tempo. (Consulte a Exibição 6)

Além das áreas de risco de segurança da estratégia de confiança zero, as organizações devem identificar os componentes individuais de cada área de risco de segurança para priorizar. Para pontos de extremidade, aplicativos, rede, dados e automação/orquestração, não há um ponto de partida claro; os profissionais de segurança variam substancialmente em quais componentes eles classificam como sua principal prioridade. No entanto, a autenticação forte normalmente é implementada primeiro para identidades, e as ferramentas de detecção de ameaças são uma prioridade clara dentro da infraestrutura. (Consulte a Exibição 7)

Exibição 6. Implementação atual da confiança zero – áreas de risco de segurança



Exibição 7. Implementação de componente de confiança zero (3 principais) - classificados como nº 1 (implementado primeiro)

Identidades	
Autenticação forte (ou seja, autenticação multifatorial, autenticação sem senha)	32%
Detecção e correção automatizada de riscos	27%
Políticas de acesso adaptativo para acessar os recursos	22%

Aplicativos	
Descoberta de Shadow IT contínua e avaliação de riscos	23%
Controle de acesso granular para seus aplicativos (como visibilidade limitada ou leitura apenas)	22%
Controle de acesso baseado em políticas para aplicativos	20%

Infraestrutura	
Acesso da equipe de operações de segurança a ferramentas de detecção de ameaças	25%
Proteção de workload na nuvem em ambientes híbridos e multinuvem	19%
Visibilidade granular e controle de acesso em todos os workloads (máquinas virtuais, servidores etc.)	17%

Automação e orquestração	
A visibilidade de ponta a ponta é estabelecida com uma plataforma centralizada de investigação e resposta	29%
Os dados de ameaças são coletados e analisados entre domínios (identidades, pontos de extremidade, aplicativos, rede, infraestrutura)	28%
A investigação e a resposta automatizadas estão habilitadas	22%

Pontos de extremidade	
Políticas/controles de prevenção contra perda de dados para todos os dispositivos não gerenciados e gerenciados	27%
Avaliação de risco de dispositivo em tempo real/detecção de ameaças de ponto de extremidade	26%
Os dispositivos são registrados com o provedor de identidade	24%

Rede	
Controles de acesso seguro para proteger as redes	25%
Proteção contra ameaças e filtragem com sinais baseados em contexto	24%
Todo o tráfego é criptografado	20%

Dados	
As decisões de acesso são regidas pelo mecanismo de política de segurança	21%
Os dados são classificados e rotulados	21%
Os arquivos mais confidenciais são protegidos persistentemente com a criptografia	20%

Não vemos isso apenas como uma série de tecnologias, mas como uma estratégia e abordagem para tratar todos os recursos de usuário, dentro ou fora de nossa rede, como não confiável até que possam ser verificados."

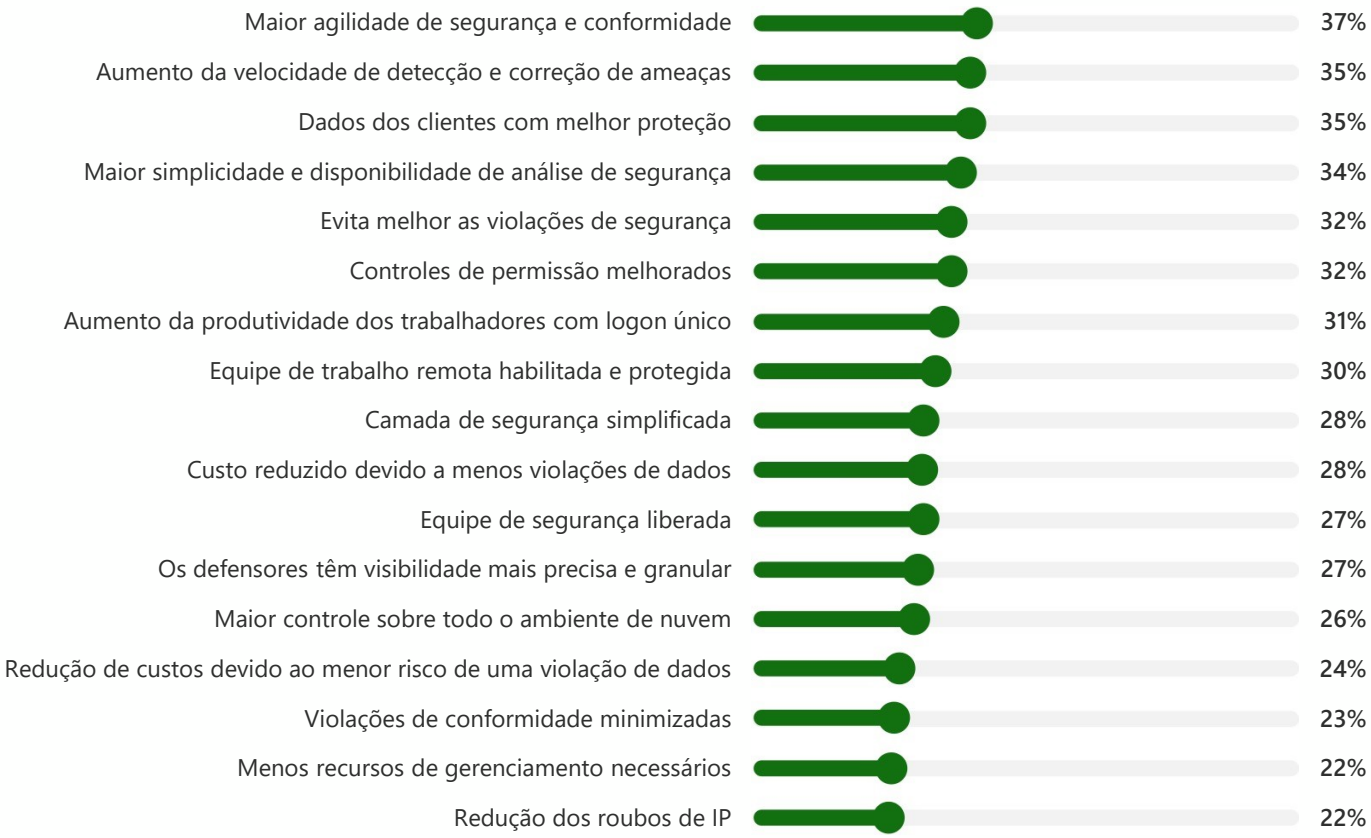
Tomadora de decisão de segurança dos EUA do setor de hotelaria

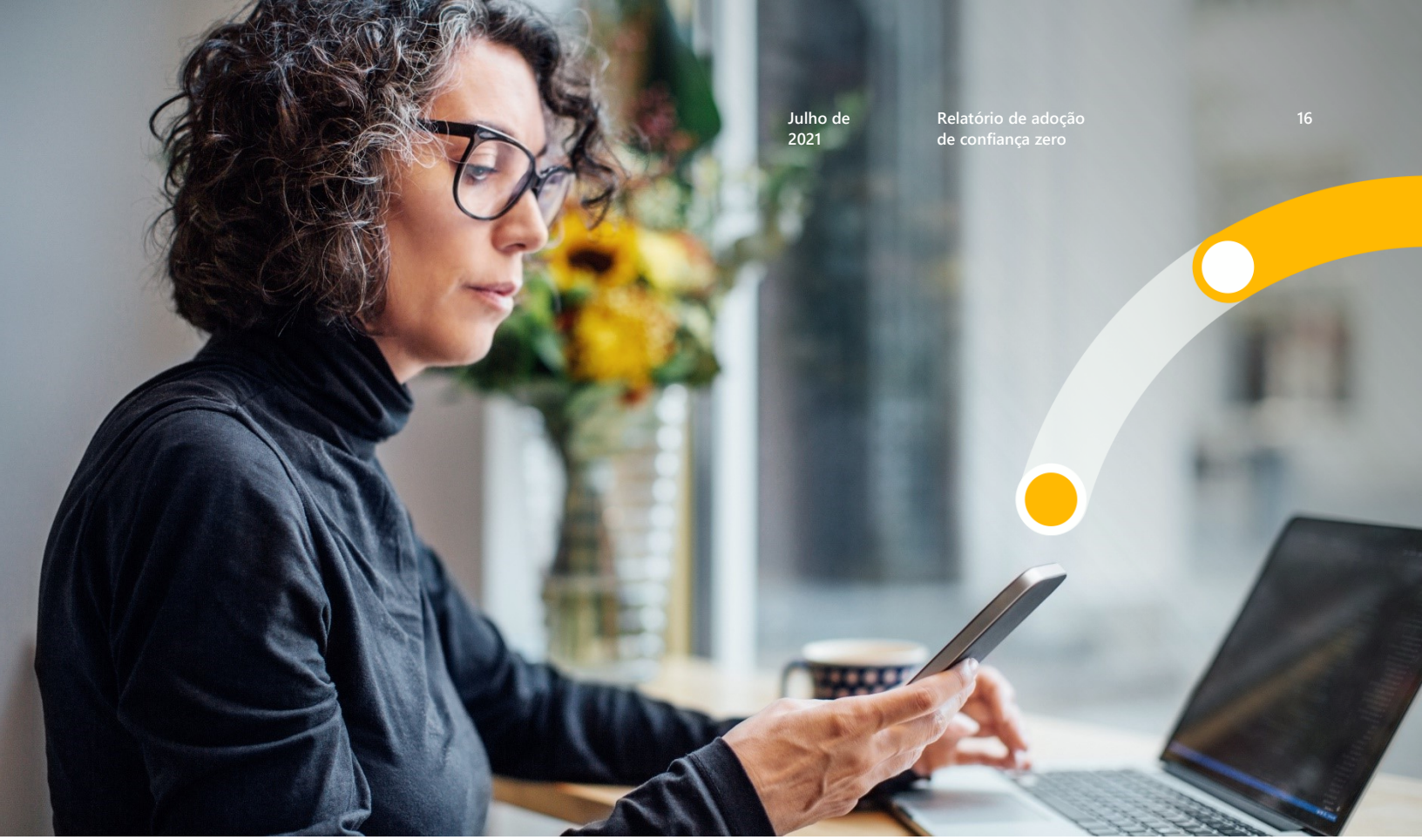
Depois que as organizações começarem a implementar uma estratégia de confiança zero, os principais benefícios incluirão maior agilidade, velocidade e proteção; as vantagens de recursos são menos comuns

Quando a estratégia de confiança zero é implementada, as organizações se beneficiam do aumento da agilidade (37%), da velocidade (35%) e da proteção dos dados do cliente (35%). (Consulte a Exibição 8) No entanto, os benefícios diretos para os funcionários, incluindo uma equipe de segurança liberada (27%) e a necessidade de menos recursos para gerenciar a infraestrutura (22%), são menos comumente realizados.

É importante ressaltar que as organizações acreditam que sua estratégia de confiança zero as ajudará a gerenciar a maioria das ameaças e mudanças no ambiente, especialmente no que diz respeito à segurança da IoT e da OT (47%).

Exibição 8. Benefícios da confiança zero





As organizações se sentem confiantes em tirar o máximo proveito da sua estratégia de confiança zero

79% sentem-se confiantes sobre sua capacidade de lidar com ameaças de segurança como um todo, embora essa confiança diminua quando a ameaça envolve a fabricação da verdade: os SDMs sentem-se menos confiantes sobre como lidar com ameaças envolvendo identidades sintéticas (20%) e deepfakes (10%).

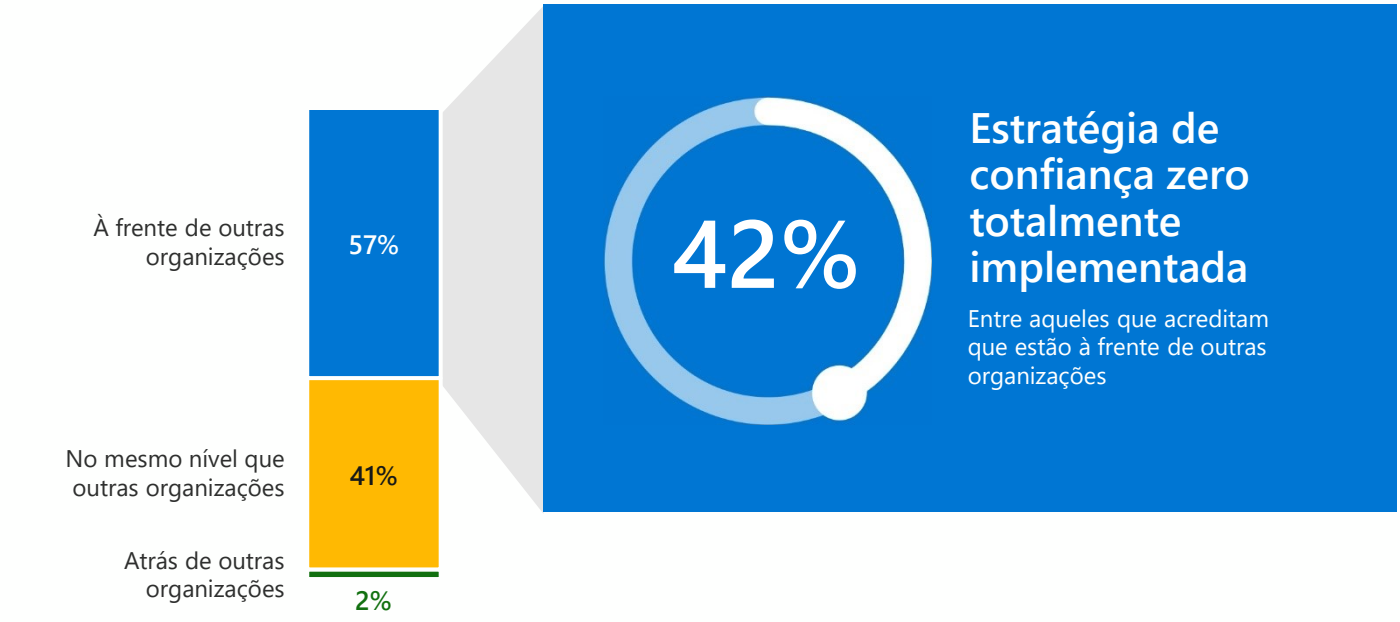
À luz dos benefícios obtidos, a confiança zero geralmente acumula associações positivas. Nos quatro mercados, os SDMs veem a abordagem de suas organizações como simultaneamente prática e aspiracional, descrevendo-a como confiante (37%) e eficiente (31%), bem como motivadora (25%), inspiradora (25%) e empolgante (25%). Especificamente no Japão, os profissionais de segurança descrevem a confiança zero como sendo exigente (27%) e transformacional (25%), sugerindo que, embora não seja fácil de implementar, seus benefícios são de longo alcance depois de adotados.

Muitos acreditam que estão à frente com a implementação da confiança zero, mas ainda falta algo

Embora apenas 35% das organizações tenham implementado totalmente sua estratégia de confiança zero, 52% dizem que estão à frente de onde planejaram estar e 57% acreditam que estão à frente de outras organizações. As organizações se consideram particularmente à frente das outras no Japão (66%) e na Austrália/Nova Zelândia (63%). Embora haja muita confiança nos mercados, parece haver um abismo entre a percepção e a realidade: entre aqueles que se sentem à frente de outras organizações, apenas 42% afirmam ter implementado totalmente uma estratégia de confiança zero. (Consulte a Exibição 9)

Embora muitas organizações estejam confiantes em sua estratégia de confiança zero e se sintam prontas para lidar com as futuras ameaças à segurança, ainda há um amplo trabalho a ser feito para implementar totalmente em áreas de risco. Entre as organizações que consideram sua estratégia de confiança zero totalmente implementada, por exemplo, quase metade não foi implementada atualmente em áreas de risco de segurança, com infraestrutura e identidades menos propensas a serem implementadas.

Exibição 9. Comparação da implementação da confiança zero



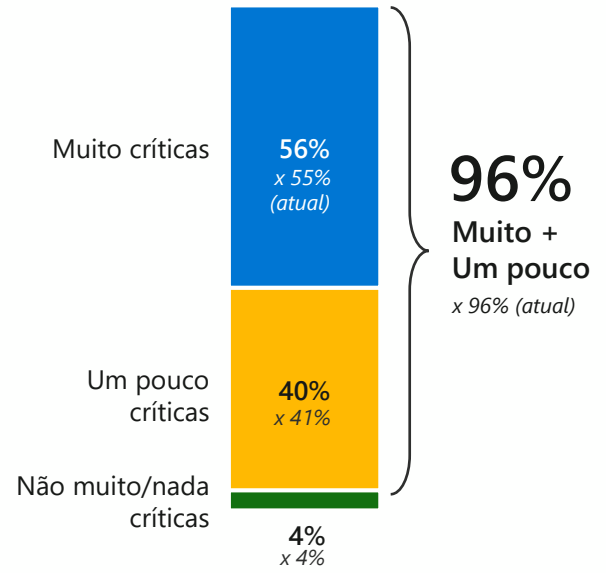
	EUA	DE	JP	AUS/NZ
À frente	59%	46%	66%	63%
No mesmo nível	40%	52%	34%	32%
Atrás	2%	2%	0%	6%

Olhando para os próximos dois anos, a estratégia de confiança zero permanecerá como prioridade de segurança

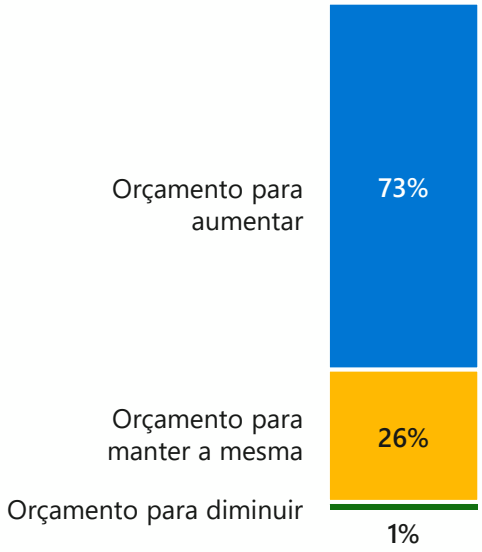
As organizações estão usando a estratégia de confiança zero, e os tomadores de decisão dizem que ela continuará sendo a principal prioridade de segurança nos próximos dois anos. A importância relativa da estratégia de confiança zero como uma iniciativa de segurança deverá aumentar (53% para 58%) em 2023, pois os SDMs antecipam que a estratégia permanecerá crítica para o sucesso geral (96%). (Consulte a Exibição 10)

A importância antecipada é particularmente alta entre as organizações japonesas, com 70% afirmando que a estratégia de confiança zero será muito crítica nos próximos dois anos em comparação com a média geral de 56%. Os orçamentos de estratégia de confiança zero também devem crescer, e 73% das organizações esperam aumentar seus orçamentos. Embora, esse número seja ligeiramente menor na Alemanha (67%), onde 31% antecipam que seus orçamentos permanecerão os mesmos. (Consulte a Exibição 11)

Exibição 10. Importância antecipada da confiança zero nos próximos dois anos

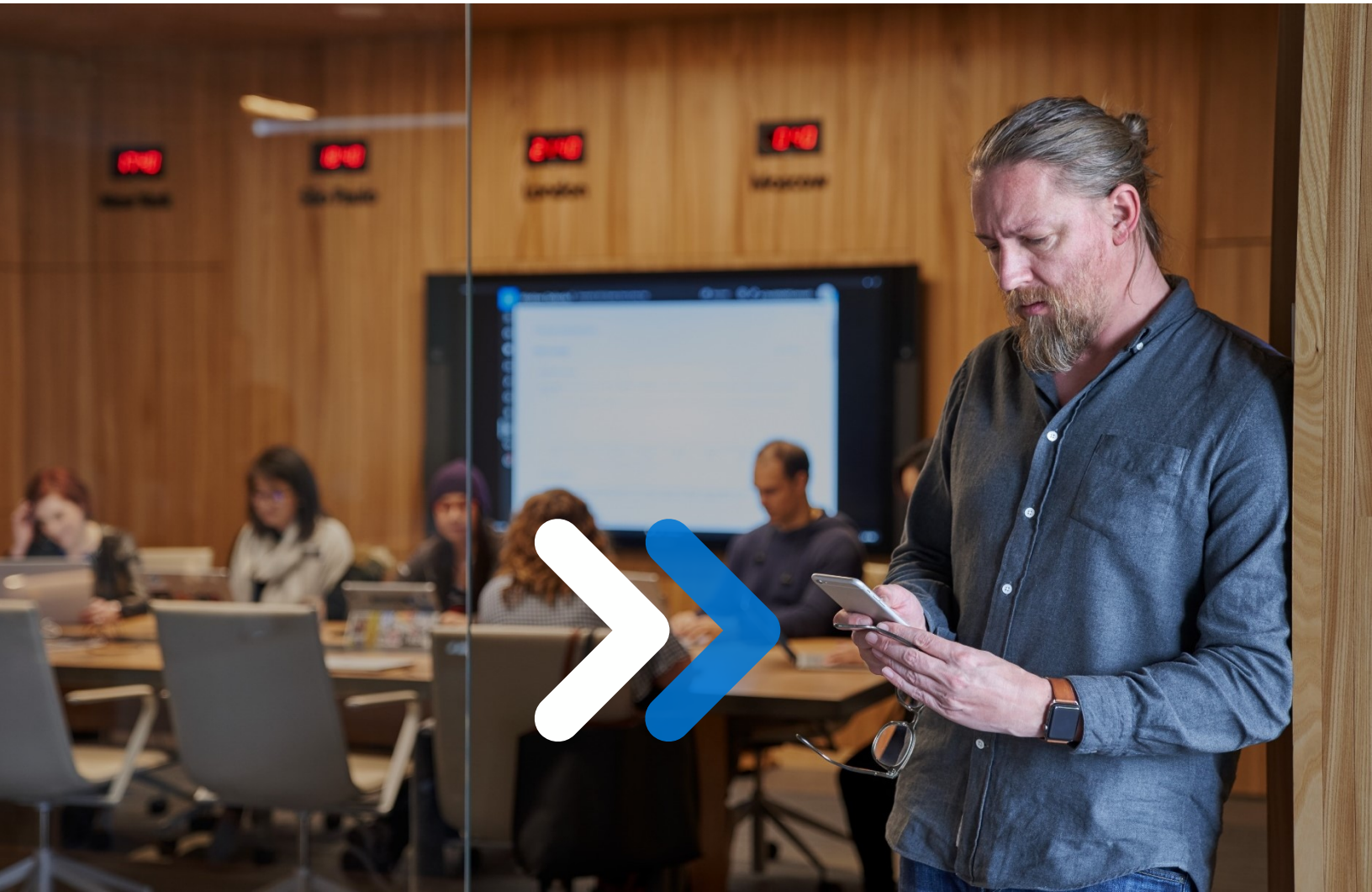


Exibição 11. Orçamento antecipado da confiança zero nos próximos dois anos



Provar que o sucesso da estratégia de confiança zero poderia impulsionar mais investimentos

As organizações que adotaram plenamente a confiança zero esperam dobrar seu investimento nos próximos dois anos, e aquelas que ainda não começaram correm o risco de ficar para trás. Essas organizações não apenas arrastam seus colegas totalmente implementados quando se trata de priorizar a confiança zero em seus planos de segurança (42% contra 66%) e antecipar aumentos orçamentários (66% x 72%), mas também sentem-se significativamente menos confiantes no gerenciamento da segurança de IoT e OT no futuro (40% vs. 53%).



Superar os desafios com os funcionários será fundamental para duplicar o investimento em confiança zero

Apesar dos rápidos avanços na adoção da estratégia de confiança zero, as organizações devem superar uma infinidade de desafios se quiserem avançar ainda mais com a implementação. (Consulte a Exibição 12) Os desafios de recursos e liderança são mais prevalentes nessas categorias. O tempo necessário para implementar estratégias de confiança zero e a falta de suporte da diretoria são as principais barreiras, sendo esta última particularmente saliente na Austrália/Nova Zelândia (65%).

Além disso, as restrições orçamentárias — que 45% das organizações identificam como uma barreira — provavelmente também desempenham um papel nos desafios de recursos e liderança.

Por exemplo, 21% dos SDMs citam dificuldades em provar o ROI de um investimento em confiança zero como uma barreira à implementação, um desafio que pode levar à falta de suporte da diretoria. Como os mercados fora dos EUA são mais propensos a ter restrições orçamentárias (60% das organizações no Japão; 57% na Alemanha; 57% na Austrália/Nova Zelândia), é possível que isso tenha um efeito cascata, levando a uma implementação mais baixa e mais lenta de estratégias de confiança zero no Japão, na Alemanha e na Austrália/Nova Zelândia em comparação com os EUA.

Exibição 12. Barreiras à confiança zero

Desafios de recursos 60%	Liderança 53%	Tecnológicas 46%	Fornecedores 46%	Restrições de orçamento 45%
20% A implementação é muito demorada	**20%** Falta suporte da maior parte da diretoria	**21%** Dificuldade em integrar soluções de segurança	**21%** Precisamos de suporte de implementação dos fornecedores	**21%** Custo de implementação de uma estratégia de confiança zero
19% Não temos gerenciamento de alterações internas	**19%** Falta suporte dos stakeholders	**19%** Incompatibilidade com sistemas herdados	**21%** Dificuldade para identificar os fornecedores certos	**21%** Dificuldade em comprovar o ROI
18% Precisamos de mais materiais de treinamento	**19%** Precisamos de ajuda para criar um caso comercial interessante	**19%** Dificuldade de escalonamento em toda a organização	**17%** Incapacidade de encontrar parceiros inovadores	**14%** Não temos um orçamento grande o suficiente
17% Não é necessário para uma organização do nosso porte	**18%** Falta apoio organizacional			
16% Não temos o talento certo para implementar corretamente				

" O apoio inicial foi desafiador, mas quando concordamos como stakeholders que investiríamos neste projeto, todos concordaram."

Tomadora de decisão de segurança dos EUA
FinTech

Os tomadores de decisão de segurança têm uma ligeira propensão a provedores holísticos ou consolidados

Quando se trata de estratégia de fornecedor de confiança zero, as organizações enfrentam a adoção da abordagem de melhor valor. A estratégia anterior envolve a compra de um conjunto de produtos para toda a arquitetura de confiança zero de um provedor holístico ou consolidado, uma solução que os SDMs acreditam que oferece mais experiência, recursos e simplicidade para aqueles que estão limitados internamente em termos de recursos. No entanto, as preocupações com essa abordagem incluem maior vulnerabilidade e falta de flexibilidade. (Consulte a Exibição 13)

A última estratégia, a melhor, envolve a obtenção de componentes individuais de tecnologia de confiança zero de fornecedores especializados. Ao contrário da melhor, essa estratégia depende de provedores que se especializam em diferentes áreas e, assim, oferecem maior flexibilidade e podem se alinhar mais estreitamente com a estratégia da organização. Dito isso, os profissionais de segurança veem a melhor como a mais cara, exigindo mais recursos e inibindo a visibilidade, desvantagens que geram desafios orçamentários e para fornecedores. (Consulte a Exibição 14)

Embora as organizações estejam em grande parte divididas, uma ligeira maioria dos SDMs (55%) prefere trabalhar com provedores holísticos (melhor valor). (As organizações na Austrália/Nova Zelândia, no entanto, se inclinam na direção oposta: 52% preferem o que há de melhor.)

Exposição 13. Benefícios e barreiras das melhores – classificados como os 2 principais

⊕ Benefícios das melhores	
O fornecedor tem especialização específica da indústria em várias soluções	24%
Mais recursos disponíveis para ajudar a planejar a estratégia de confiança zero	23%
Camada de segurança simplificada	22%

⊖ As desvantagens das melhores	
A dependência de um único fornecedor aumenta a vulnerabilidade	34%
Requer uma integração mais complexa com a arquitetura herdada	33%
Menos flexibilidade para o funcionamento especializado	29%

Exposição 14. Benefícios e barreiras das melhores – classificados como os 2 principais

⊕ Benefícios das melhores	
Flexibilidade para buscar as melhores soluções para qualquer componente da estratégia de confiança zero	33%
Pode alinhar mais de perto a solução com a arquitetura ou a estratégia da minha organização	30%
Maior oportunidade de inovação com vários fornecedores	26%

⊖ As desvantagens das melhores	
Custos mais elevados	29%
Incapacidade de compartilhar dados entre diferentes soluções	26%
Alto volume de soluções para equipes internas adotarem e gerenciarem	26%

Considerações finais

À medida que os riscos de segurança se tornam mais frequentes e nefastos, as organizações de todos os mercados e indústrias optam por uma estratégia de confiança zero que nos guia a "nunca confiar, sempre verificar." A estratégia de confiança zero é a principal prioridade de segurança para as organizações que visam melhorar sua postura geral de segurança, experiência do usuário final e produtividade, simplificar os procedimentos de segurança para os funcionários e reduzir os custos. No entanto, embora os benefícios de uma estratégia de confiança zero estejam bem estabelecidos, os recursos limitados e o ceticismo entre a liderança estão no caminho da implementação universal.

A adoção da estratégia de confiança zero acelerou nos últimos três anos, em parte devido à pandemia de COVID-19. Fundamentalmente, a mudança para locais de trabalho remotos e híbridos está impulsionando uma adoção mais ampla de abordagens de confiança zero, que prometem proteger sistemas e dados, mesmo quando os funcionários os acessam fora do local, às vezes em dispositivos pessoais. A adoção acelerada devido à COVID é um bom indicador da preparação da confiança zero em geral, com organizações que adotaram a estratégia durante a pandemia, tendo implementado em mais áreas de risco de segurança do que seus colegas.

Dito isso, até mesmo os adotantes de estratégia d e confiança zero mais avançados têm trabalho a fazer, e as percepções errôneas das organizações em torno de sua própria maturidade de confiança zero podem deixar algumas com vulnerabilidades que nem sabem que têm.

A maioria das organizações em todos os mercados acredita que a importância de uma estratégia de confiança zero só crescerá com o tempo e espera que os orçamentos aumentem. Essa mudança antecipada na priorização é particularmente crucial para os mercados de fora dos EUA, onde as preocupações orçamentárias são barreiras salientes para a adoção. Esforçar-se para uma implementação completa pode ser complicado em termos financeiros e logísticos. Ainda assim, os benefícios de uma abordagem de confiança Zero são inegáveis, e a Microsoft estará lá para orientar e apoiar as organizações à medida que elas embarcam nessa fronteira em expansão.

Para saber mais sobre a confiança zero e fazer uma avaliação da maturidade da confiança zero da sua organização, acesse

aka.ms/zerotrust

Objetivos detalhados de pesquisa e recrutamento de público-alvo

Os objetivos da pesquisa incluíram:

Entender o estado atual das abordagens de confiança zero

Descobrir mentalidades, práticas recomendadas, benefícios e desafios da adoção de abordagens de confiança zero

Explorar o futuro das abordagens de confiança zero

Contextualizar inovações e tendências em abordagens de confiança zero

Para atender aos critérios de triagem, os tomadores de decisão de segurança precisavam ser:

Responsáveis pela segurança em sua organização, incluindo segurança cibernética, operações de segurança, proteção contra ameaças, gerenciamento de identidades, gerenciamento de riscos, segurança de aplicações, perícia digital e resposta a incidentes

Empregado em tempo integral em uma empresa de nível corporativo (mais de 1.000 funcionários nos EUA; mais de 500 funcionários na Alemanha/Japão/Austrália/Nova Zelândia)

Idades entre 25 e 75

Familiarizado com a confiança zero

Envolvidos na tomada de decisão para desenvolvimento/implementação de estratégia de confiança zero

Dos 911 tomadores de decisão de segurança entrevistados para a pesquisa da Wave em abril de 2021:

Nos EUA, 477 SDMs foram entrevistados

Na Alemanha, 201 SDMs foram entrevistados

Na Austrália/Nova Zelândia, 126 SDMs foram entrevistados

No Japão, 107 SDMs foram entrevistados

Observação: a pesquisa foi realizada durante a pandemia mundial de COVID-19, que estava em diferentes estágios de escalonamento/contenção