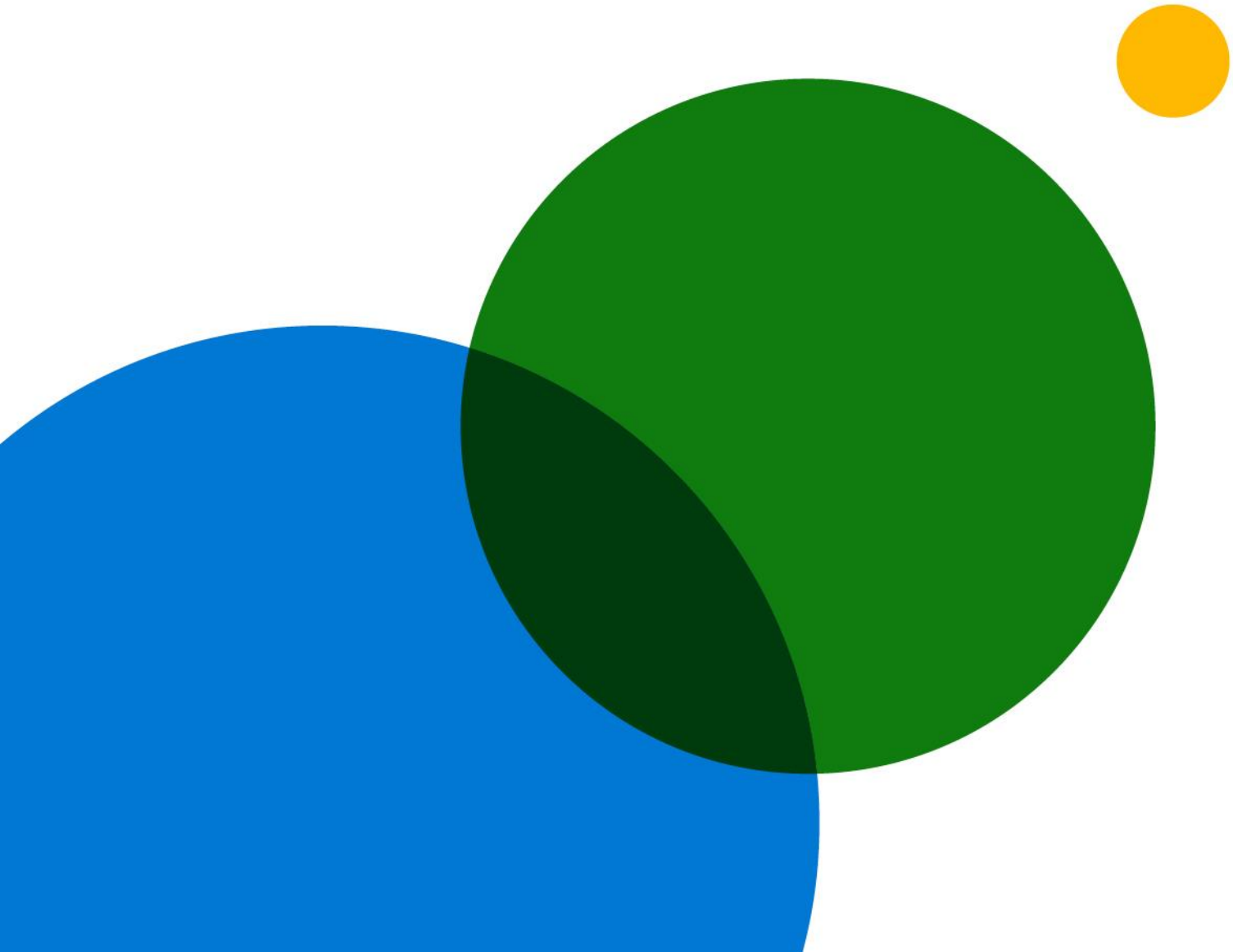
Microsoft Security

hypothesis

Relatório de adoção Confiança Zero



Índice

03
Introdução

04
Metodologia

05
Coisas a saber sobre a adoção da Confiança Zero

06
Com quem falámos

07
Aprendizagens globais da investigação

24
Objetivos de investigação detalhados e recrutamento de público

Introdução

Vasu Jakkal / Vice-Presidente Corporativo, Segurança, Conformidade e Identidade

Este último ano foi notável na evolução da cibersegurança e na ascensão da Confiança Zero como estratégia de orientação para a nossa indústria e organizações em todo o mundo.

No início da pandemia, o local de trabalho tornou-se quase totalmente remoto de um dia para o outro. Esta mudança forçou muitas organizações a adaptarem-se rapidamente para apoiar os colaboradores que estavam a fazer o trabalho como podiam: utilizando dispositivos pessoais, colaborando através de serviços na cloud e partilhando dados fora do perímetro da rede corporativa. À medida que as organizações se adaptavam a esta transformação, também enfrentavam cibercriminosos cada vez mais sofisticados que evoluem continuamente os seus alvos, táticas e recursos.

Hoje, o trabalho híbrido é a nova realidade. Neste contexto, e face à rápida mudança, as organizações por nós inquiridas disseram-nos que confiam na Confiança Zero para maior segurança e agilidade no cumprimento, maior rapidez na deteção e resposta a ameaças, e maior simplicidade e disponibilidade de análises de segurança..

Baseada nos princípios de verificação explícita, utilizar o acesso menos privilegiado, e assumir a violação, uma arquitetura de Confiança Zero abrangente cria salvaguardas dentro e através da identidade, pontos finais, aplicações, infraestrutura, rede e dados, juntamente com uma maior visibilidade, automatização e orquestração. Não só recomendamos esta abordagem com os nossos clientes e parceiros: adotamo-la na nossa abordagem à segurança global e ao desenvolvimento de software aqui na Microsoft..

Este relatório elucida o caminho da adoção da Confiança Zero em diversos mercados e indústrias. Esperamos que os conhecimentos resultantes desta investigação possam ajudar a acelerar a sua própria adoção da estratégia de Confiança Zero, lançar luz sobre o progresso coletivo dos seus pares, e fornecer insights sobre o estado futuro deste espaço em rápida evolução.

Metodologia

A Microsoft encomendou ao Hypothesis Group, uma agência de insights, design e estratégia, a execução do Relatório de Adoção de Confiança Zero e investigação. A investigação incluiu duas fases nos EUA para destacar tendências e dinâmica na adoção da Confiança Zero, com mercados adicionais acrescentados na segunda fase para descobrir tendências globais.

A investigação inicial ocorreu em agosto de 2020, quando foi realizado um inquérito online de 15 minutos nos EUA com 300 security decision-makers (SDM) envolvidos nas decisões estratégicas da Confiança Zero nas empresas de uma série de indústrias. Para além do inquérito online, foram realizadas cinco entrevistas em profundidade online em setembro de 2020 entre os SDM dos EUA numa série de indústrias.

Em abril de 2021, foi realizada a investigação global nos EUA, Alemanha, Japão e Austrália/Nova Zelândia através de um grupo semelhante de security decision-makers. Mais de 900 participantes fizeram um inquérito online de 15 minutos com perguntas sobre a adoção da sua estratégia de Confiança Zero, melhores práticas, benefícios, desafios, e como pretendem investir no futuro.

Coisas a saber sobre a adoção da Confiança Zero

01 / As organizações estão prontas para capitalizar a estratégia da Confiança Zero, acelerada pela mudança para um local de trabalho híbrido e pela Covid-19

Os security decision-makers (SDM) dizem que o desenvolvimento de uma estratégia de confiança zero é a sua prioridade de segurança número 1, com 96% a afirmar que é fundamental para o sucesso da sua organização. Os principais incentivos para a adoção de uma estratégia de Confiança Zero são para melhorar a sua postura de segurança global e a experiência do utilizador final. A mudança para um local de trabalho híbrido, acelerada pela COVID-19, está também a conduzir a uma adoção mais ampla da estratégia da Confiança Zero: 81% das organizações empresariais iniciaram a mudança para um local de trabalho híbrido, com 31% totalmente feita. No entanto, 94% têm preocupações sobre a transição, principalmente, o uso indevido dos colaboradores, o aumento da workloads das TI, e os ciberataques. Tendo isto em conta, as considerações-chave para uma estratégia incluem o aumento da formação dos colaboradores e a autenticação multifator (AMF) para assegurar uma experiência e transição suave para o utilizador.

02 / A estratégia de Confiança Zero permite flexibilidade onde as organizações podem começar a implementação para adaptar a abordagem às suas necessidades

Menos de 15% das organizações começaram a implementar a estratégia de Confiança Zero na mesma área de risco de segurança. Isto deve-se em grande parte ao facto de a implementação ser abordada como um processo de ponta a ponta entre pilares e capacidades da arquitetura de segurança, e não como uma série de tecnologias individuais e díspares. Do mesmo modo, a ordem pela qual os componentes individuais da Confiança Zero dentro de uma área de risco de segurança são implementados é altamente variável, com os profissionais de segurança a diferirem substancialmente em que componentes começam a implementar primeiro.

03 / Embora a estratégia da Confiança Zero seja amplamente adotada e melhore a capacidade das organizações para gerir as ameaças, ainda há trabalho a ser feito

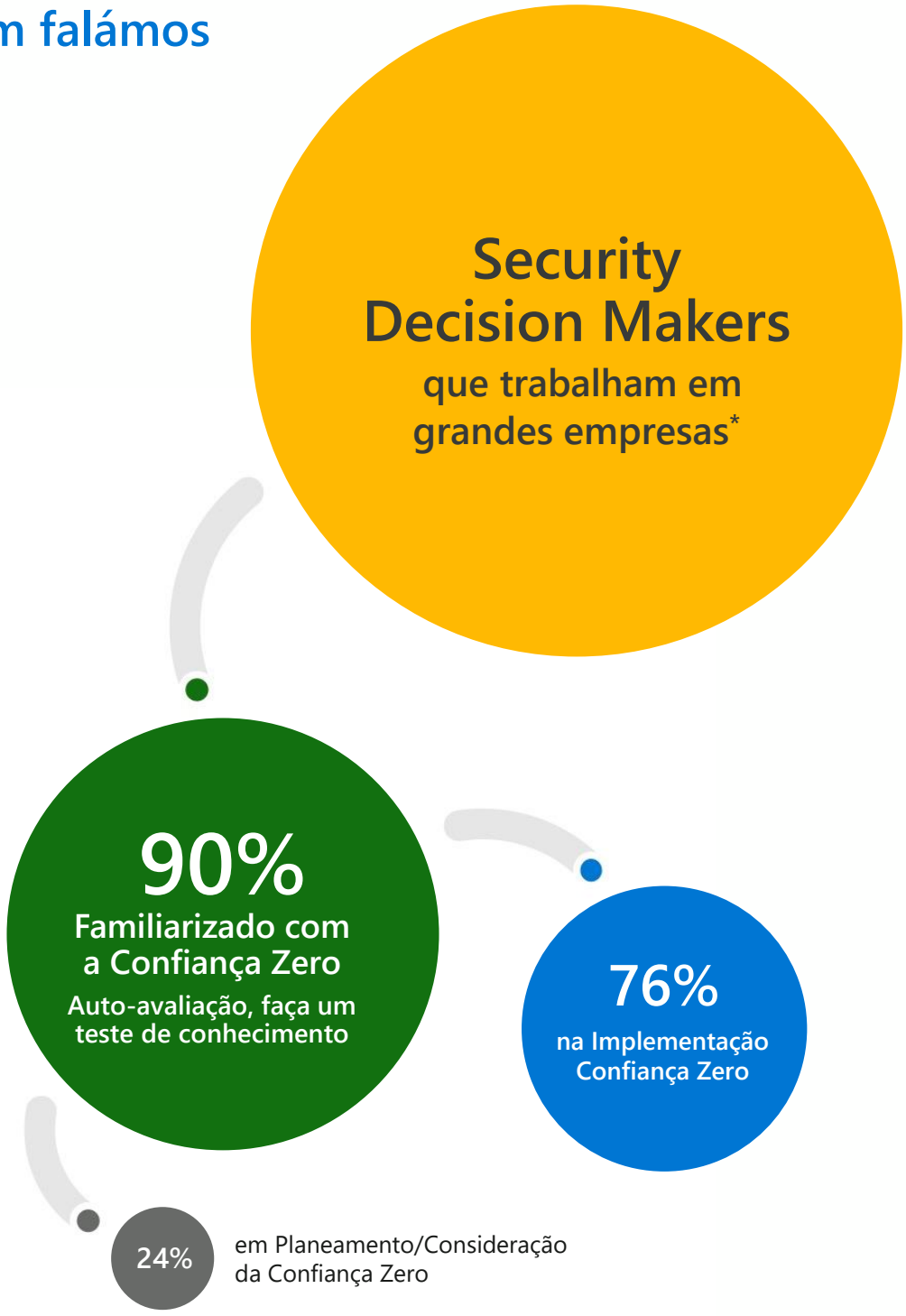
76% das organizações começaram pelo menos a implementar uma estratégia de Confiança Zero, com 35% a afirmar a sua plena implementação. No entanto, os que afirmam ter uma implementação plena admitem não ter acabado de implementar a estratégia de Confiança Zero em todas as áreas e componentes de risco de segurança. A estratégia de Confiança Zero é convincente porque proporciona maior agilidade, rapidez na deteção de ameaças e melhor capacidade de gerir a segurança da Internet das Coisas (IoT) e da Tecnologia Operacional (OT). A adoção está a crescer nos EUA (70% em agosto de 2020 para 79% em abril de 2021); os EUA também estão mais avançados na implementação da Confiança Zero em relação a outros países que começaram a adotá-la mais tarde e as organizações nos EUA afirmam estar menos limitadas pelos orçamentos. No entanto, enquanto 57% das organizações afirmam estar à frente de outras quando se trata de adoção, cerca de metade ainda tem mais trabalho a fazer, uma vez que ainda não implementaram totalmente a Confiança Zero em todas as áreas e componentes de risco de segurança.

04 / Olhando para o futuro, a estratégia de Confiança Zero continuará a ser uma prioridade máxima e exigirá uma tomada de decisão cuidadosa quando se trata de colaboradores e de fornecedores

Espera-se que a estratégia Confiança Zero continue a ser a prioridade número 1 em matéria de segurança daqui a dois anos e as organizações preveem aumentar o seu investimento. Ultrapassar os desafios com os seus colaboradores (incluindo o pessoal das equipas de segurança e a adesão da liderança) será a chave para duplicar o investimento da Confiança Zero. Quando se trata da estratégia de fornecedores, os security decision-makers têm uma ligeira preferência por trabalhar com fornecedores holísticos ou consolidados, dado que a seleção de fornecedores está muitas vezes dependente da disponibilidade de especialização interna. Os benefícios da abordagem best-in-suite incluem uma maior especialização, recursos e simplicidade, embora possa demorar mais tempo a implementar, ser mais difícil de integrar na arquitetura de segurança existente, e aumentar a vulnerabilidade potencial. existente, e aumentar a vulnerabilidade potencial.

Com quem falámos

Global



*Mais de 1000 colaboradores nos EUA; mais de 500 colaboradores na Alemanha, Japão, Austrália/Nova Zelândia

Aprendizagens globais da investigação

As organizações estão prontas para capitalizar a estratégia da Confiança Zero

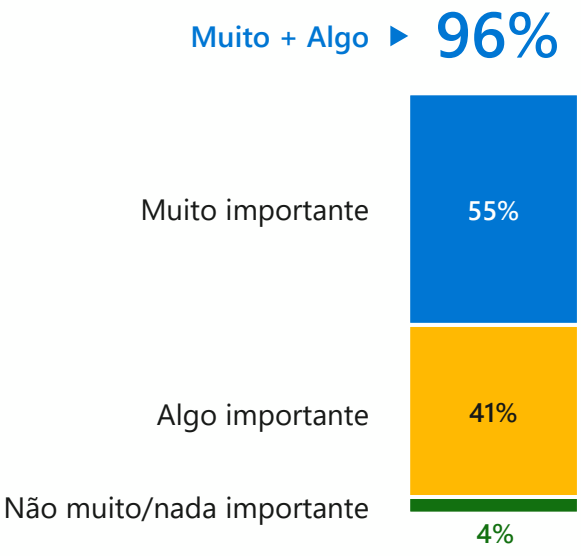
A estratégia de Confiança Zero é hoje a prioridade número 1 em segurança entre mercados e indústrias, com várias organizações a adotarem uma estratégia de Confiança Zero nos últimos anos. Embora a Confiança Zero esteja no topo das prioridades para todos (53%), é uma prioridade particularmente alta para organizações nos Estados Unidos (56%) e na Alemanha (53%).

Quase todos os profissionais de segurança (96%) acreditam que uma estratégia de Confiança Zero é importante para o sucesso da sua organização. (Ver Anexo 1) Além de reforçar a sua postura global de segurança e melhorar a experiência do utilizador final, os profissionais de segurança procuram uma estratégia de Confiança Zero para simplificar os procedimentos de segurança dos colaboradores. (Ver Anexo 2)

Como explica um security decision-maker dos EUA no setor da Hospitalidade, *"O objetivo é melhorar a nossa postura de segurança em geral, mas tem tudo a ver com reduzir o atrito na experiência do utilizador final e facilitar-lhe a vida."*

Além disso, 31% dos profissionais de segurança veem a estratégia Confiança Zero como uma ferramenta importante na mudança iminente para um local de trabalho híbrido pós-pandémico; este fator é particularmente evidente na Austrália/Nova Zelândia (44%).

Anexo 1. A Confiança Zero é importante



Prova 2. Motivadores Confiança Zero

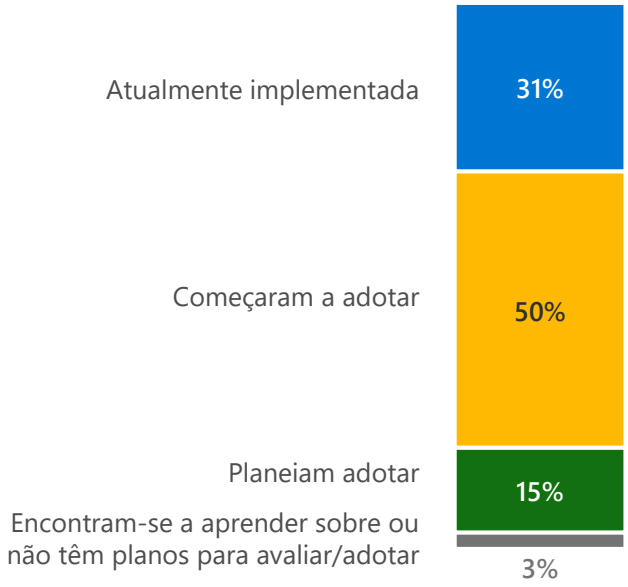
Principais Motivadores	
Melhorar a postura de segurança global	47%
Melhorar a experiência e produtividade do utilizador final	44%
Transformar a forma como as equipas de segurança trabalham em conjunto	38%
Simplificar o stack de segurança	35%
Reduzir os custos de segurança	35%

A mudança para um local de trabalho híbrido está a impulsionar a adoção mais ampla da estratégia Confiança Zero

81% das organizações empresariais iniciaram a mudança para um local de trabalho híbrido, com 31% já totalmente adotados. Dito isto, as taxas de adoção plena são inconsistentes entre os mercados: enquanto a Austrália e a Nova Zelândia lideram com 37%, a Alemanha está muito atrasada, com apenas 20% das organizações já tendo mudado para um modelo híbrido. (Ver Anexo 3)

Mesmo com os mercados globais a avançarem para um local de trabalho híbrido a taxas díspares, a grande maioria (91%) das organizações que ainda não completaram a transição antecipam fazê-lo nos próximos cinco anos. Crucialmente, 94% estão preocupados com a transição, com o uso indevido dos colaboradores, o aumento das workloads das TI e o aumento do risco de ciberataques a encabeçarem a lista de preocupações. (Ver Anexo 4)

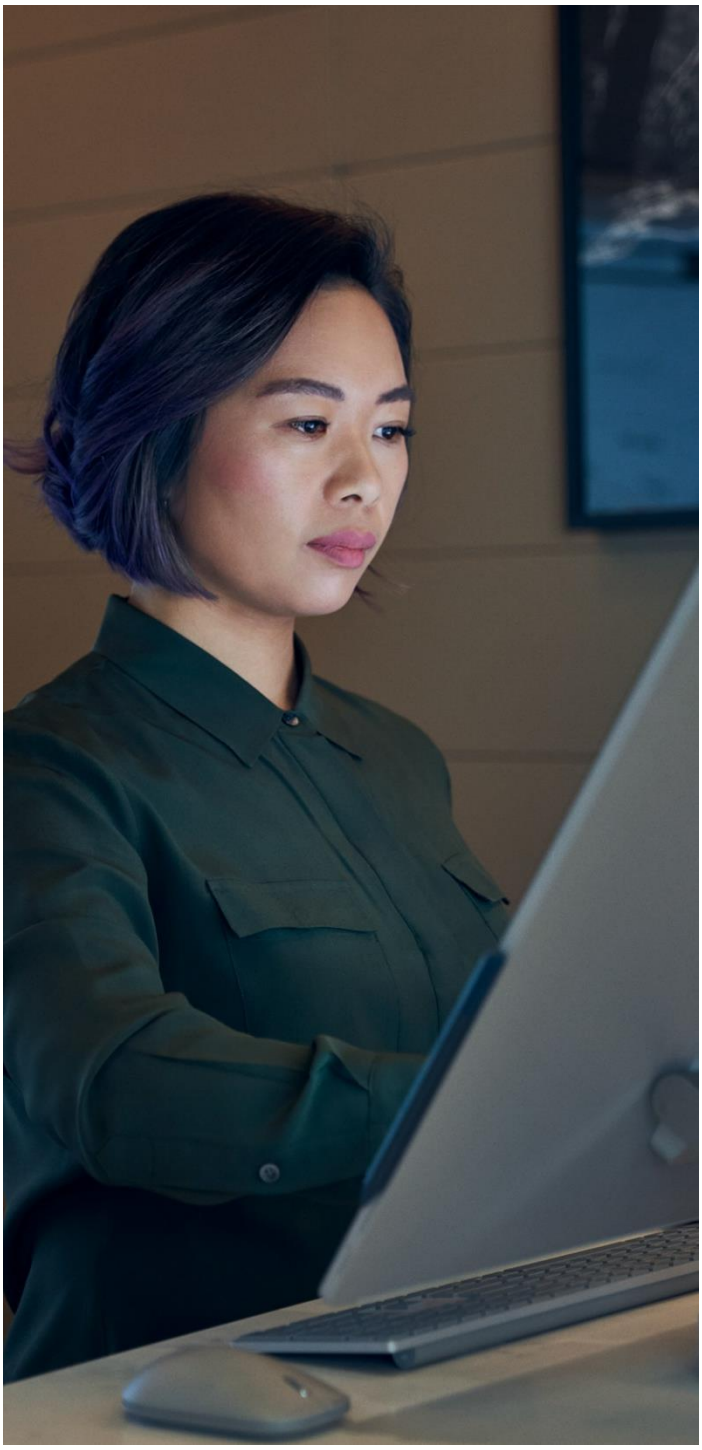
Anexo 3. Intenção de trabalho híbrido



Anexo 4. Preocupações de trabalho híbrido

Download de aplicações não seguras pelo colaboradores	37%
Um aumento da workload de TI	37%
Ataques de ransomware	36%
Ataques de phishing	35%
Utilização inadequada de dispositivos pessoais	34%
Acesso a dados não autorizado	31%
Incapacidade de gerir todos os dispositivos	30%
Utilização de contas de email pessoais	30%
Incumprimento dos regulamentos de dados	24%

A Covid-19 trouxe novas considerações que aceleram a mudança para a estratégia da Confiança Zero



Num esforço para minimizar potenciais problemas, as partes interessadas sublinham a importância de uma maior formação dos colaboradores (54%) (particularmente no Japão (61%) e Alemanha (58%)) e autenticação multifator (AMF) (50%) (particularmente nos Estados Unidos (52%) e Alemanha (56%)) para assegurar uma experiência e transição suaves aos utilizadores.

Uma vez que o trabalho seguro à distância e híbrido pode ser auxiliado pela estratégia Confiança Zero, a COVID-19 acelerou a adoção de uma estratégia Confiança Zero para 72% das organizações, embora hajam assimetrias 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 mais baixas na Alemanha (62%), talvez devido a uma transição mais lenta para um local de trabalho híbrido.

A Confiança Zero está amplamente implementada em todo o mundo e a crescer nos EUA

A Confiança Zero não é apenas uma palavra na moda; é uma realidade. 76% das organizações começaram, pelo menos, a implementar esta estratégia e 35% acreditam que a sua implementação é plena. No entanto, estes dados pintam um quadro demasiado otimista, uma vez que muitas organizações que consideram a sua implementação plena não terminaram, na sua própria admissão, de lidar com a execução em todas as áreas de risco de segurança. Atualmente, os EUA estão à frente na adoção da estratégia Confiança Zero em relação a outros mercados e continua a crescer rapidamente: em comparação com agosto de 2020, a implementação da estratégia Confiança Zero nos EUA aumentou de 70% para 79%, um salto considerável em apenas oito meses.
(Ver Anexo 5)

Embora a estratégia Confiança Zero predomine atualmente no espaço de segurança, a sua ubiquidade é relativamente nova. 82% das empresas implementaram estratégias de Confiança Zero nos últimos três anos, com 21% a fazê-lo nos últimos 12 meses. Dito isto, 26% das organizações americanas começaram 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. Esta implementação anterior nos EUA - em conjunto com menos restrições orçamentais - pode ajudar a explicar porque é que as organizações nos EUA estão à frente na adoção da Confiança Zero em comparação com organizações de outros mercados. Numa linha semelhante, a relativa incipiência da Confiança Zero na Alemanha ajuda a contextualizar as suas taxas de adoção mais baixas: 97% das organizações alemãs só iniciaram a sua implementação nos últimos três anos.

Anexo 5. Implementação Confiança Zero

	EUA (2020)	EUA	Alemanha	Japão	Austrália/ Nova Zelândia
Implementação Confiança Zero	70%	79%	75%	76%	71%
• Totalmente implementada	27%	44%	19%	32%	28%
• Em curso	43%	35%	56%	44%	43%

35% com implementação plena

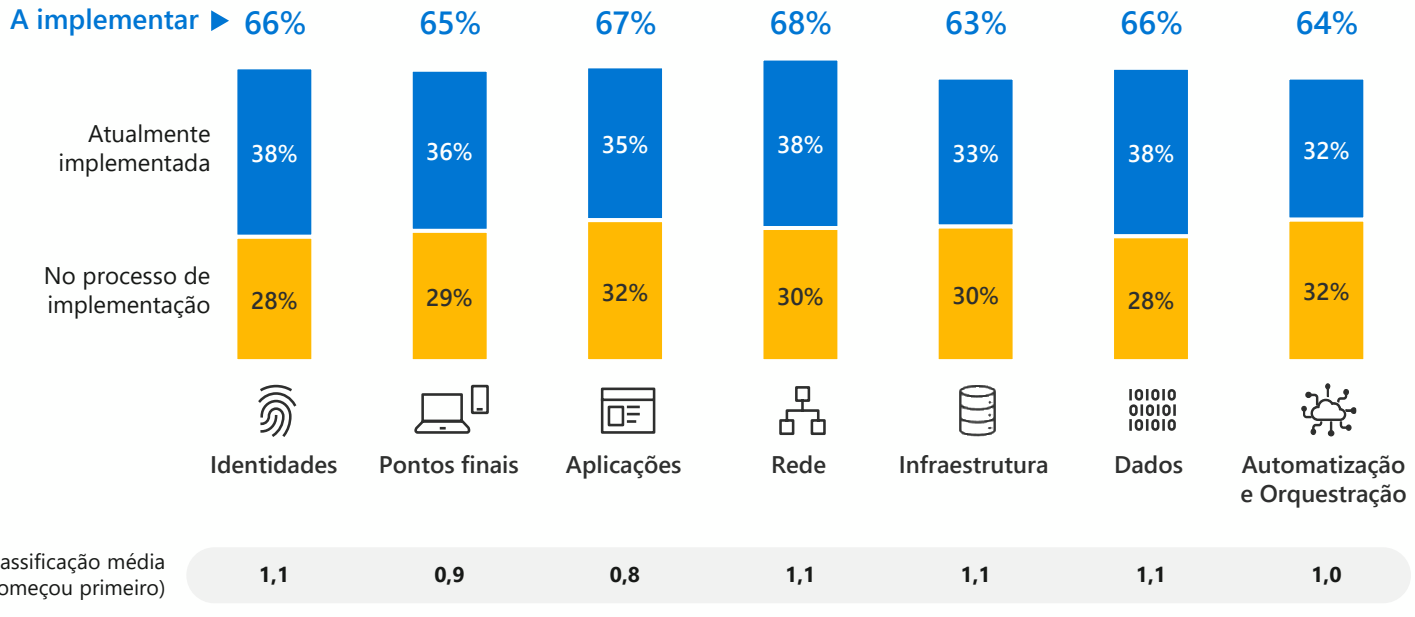
42% com implementação em curso

Não há uma abordagem única para a implementação da Confiança Zero, permitindo o seu início em qualquer lugar

Nenhuma área de risco de segurança única (Identidades, Endpoints, Aplicações, Rede, Infraestrutura, Dados, Automatização e Orquestração) se destaca como ponto de partida primário para a estratégia da Confiança Zero, uma vez que menos de 15% começam com a mesma área de risco de segurança. As organizações estão a começar em diferentes locais, provavelmente com base nas suas necessidades e recursos internos disponíveis. Eventualmente, procuram adotar a estratégia de Confiança Zero em todas as áreas de risco de segurança para assegurar ainda mais proteção contra ameaças, pelo que a Confiança Zero é vista como uma estratégia de ponta a ponta a ser completada ao longo do tempo. (Ver Anexo 6)

Para além das áreas de risco de segurança da estratégia da Confiança Zero, as organizações devem identificar as componentes individuais de cada área de risco de segurança a priorizar. Para endpoints, aplicações, rede, dados e automatização/orquestração, não existe um ponto de partida claro; os profissionais de segurança variam substancialmente nos componentes que classificam como a sua prioridade máxima. Contudo, a autenticação forte é tipicamente implementada primeiro para Identidades, e as ferramentas de deteção de ameaças são uma prioridade clara dentro da Infraestrutura. (Ver Anexo 7)

Anexo 6. Implementação atual da Confiança Zero - Áreas de risco de segurança



Anexo 7. Implementação da componente Confiança Zero (Top 3) - Classificado nº1 (Implementado primeiro)

Identidades	
Autenticação forte (i.e., autenticação multifator, autenticação sem palavras-passe)	32%
Deteção e reparação automatizada de riscos	27%
Políticas de acesso adaptativo ao acesso ao portal de acesso aos recursos	22%

Aplicações	
Descoberta contínua da TI sombra e avaliação de risco	23%
Controlo de acesso granular às suas aplicações (como visibilidade limitada ou apenas leitura)	22%
Controlo de acesso baseado em políticas para aplicações	20%

Infraestrutura	
Acesso da equipa de operações de segurança a ferramentas de deteção de ameaças	25%
Proteção da workload em contexto híbrido e multi-cloud	19%
Visibilidade granular e controlo de acessos em todas as workloads (máquinas virtuais, servidores, etc.)	17%

Automatização e Orquestração	
A visibilidade de ponta a ponta é estabelecida com uma plataforma centralizada de investigação e resposta	29%
Os dados de ameaça são recolhidos e analisados em domínios (identidades, endpoints, aplicações, rede, infraestrutura)	28%
Investigação e resposta automatizadas estão ativadas	22%

Pontos finais	
Políticas/controlos de prevenção de perdas de dados para todos os dispositivos não geridos e geridos	27%
Avaliação do risco do dispositivo em tempo real / deteção de ameaças de endpoint	26%
Os dispositivos estão registados com o fornecedor de identidade	24%

Rede	
Controlos de acesso seguros para proteger redes	25%
Proteção e filtragem de ameaças com sinais baseados em contexto	24%
Todo o tráfego está encriptado	20%

Dados	
As decisões de acesso são regidas pelo motor da política de segurança	21%
Os dados são classificados e rotulados	21%
Os ficheiros mais sensíveis são persistentemente protegidos com encriptação	20%

Não o encarámos apenas como uma série de tecnologias, mas como uma estratégia e abordagem para tratar cada recurso do utilizador, seja dentro ou fora da nossa rede, como não confiável até que pudessem ser verificados".

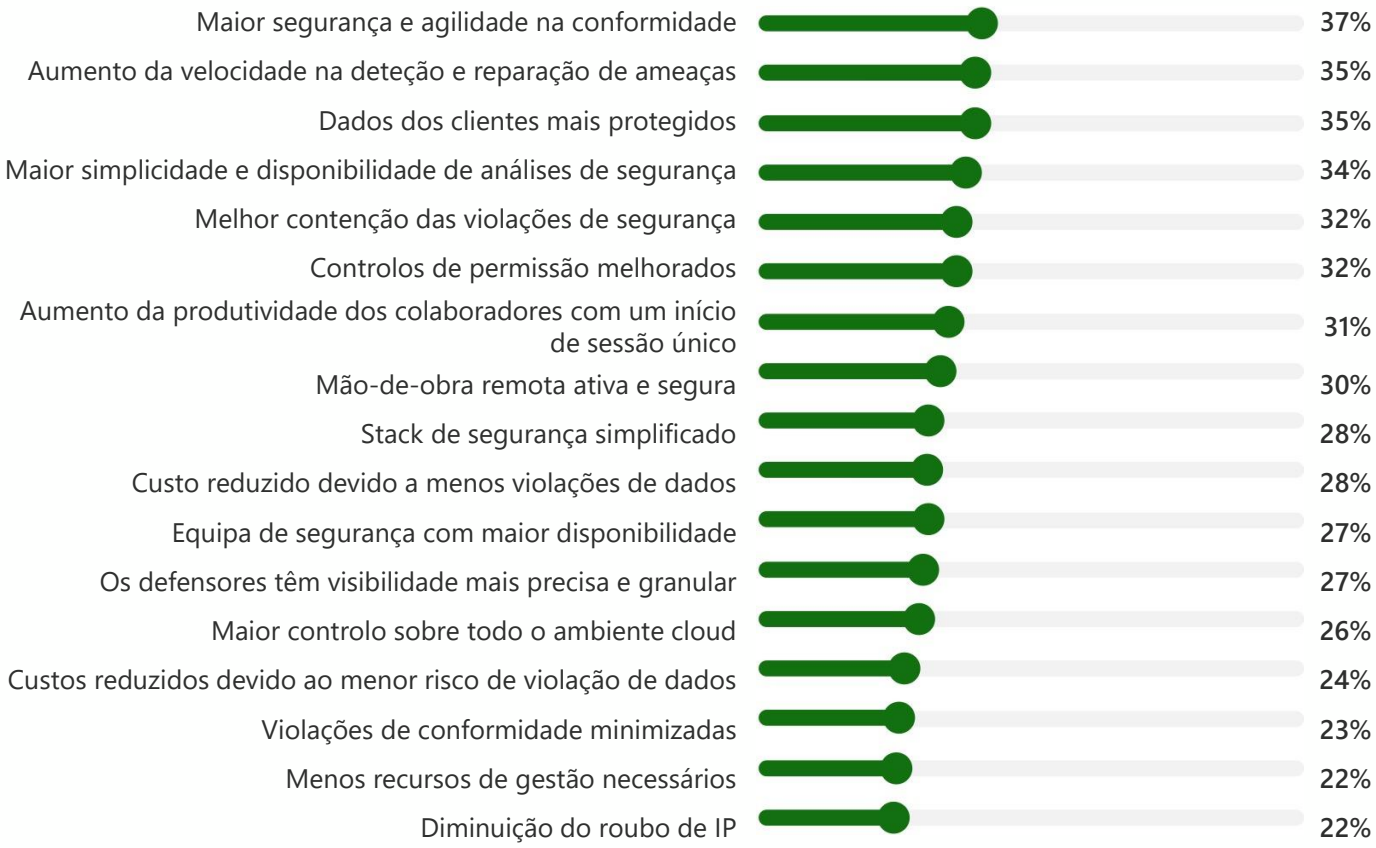
Security Decision-Maker dos EUA
Hospitalidade

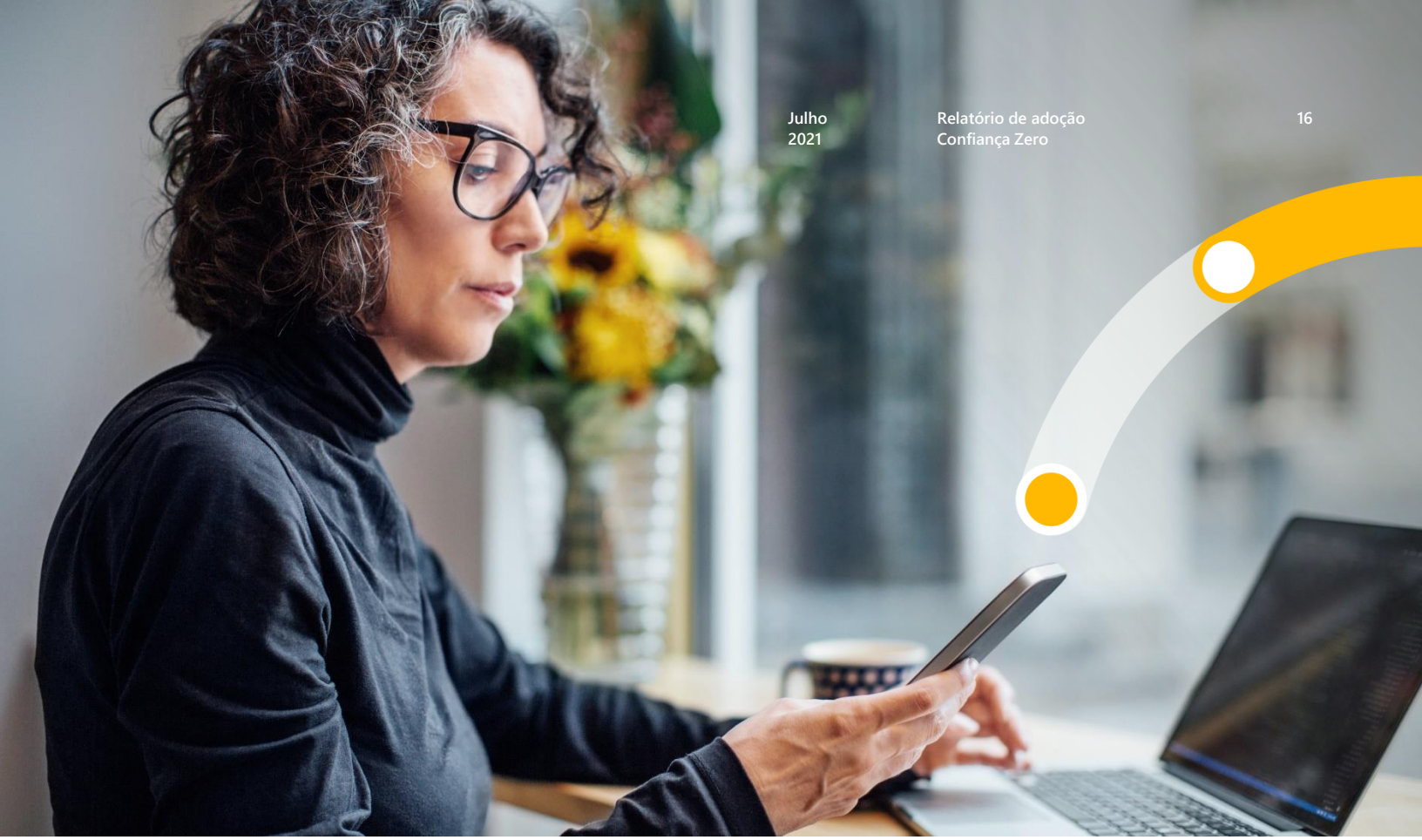
Assim que as organizações começam a implementar uma estratégia de Confiança Zero, os principais benefícios incluem maior agilidade, rapidez e proteção; as vantagens em termos de recursos são menos comuns

Uma vez implementada a estratégia Confiança Zero, as organizações beneficiam de maior agilidade (37%), rapidez (35%), e proteção dos dados dos clientes (35%). (Ver Anexo 8) No entanto, os benefícios diretos para os colaboradores, incluindo uma equipa de segurança libertada (27%) e a necessidade de menos recursos para gerir a infraestrutura (22%), são menos comumente alcançados.

É importante que as organizações acreditem que a sua estratégia Confiança Zero as irá ajudar a gerir a maioria das ameaças e alterações ao ambiente, especialmente no que diz respeito à segurança IoT e OT (47%).

Anexo 8. Benefícios da Confiança Zero





As organizações sentem-se confiantes em tirar o máximo partido da sua estratégia de Confiança Zero

79% sentem-se confiantes quanto à sua capacidade de lidar com as ameaças à segurança como um todo, embora esta confiança diminua quando a ameaça envolve uma falsificação da verdade: os SDM sentem-se menos confiantes quanto a lidar com ameaças envolvendo identidades sintéticas (20%) e deepfakes (10%).

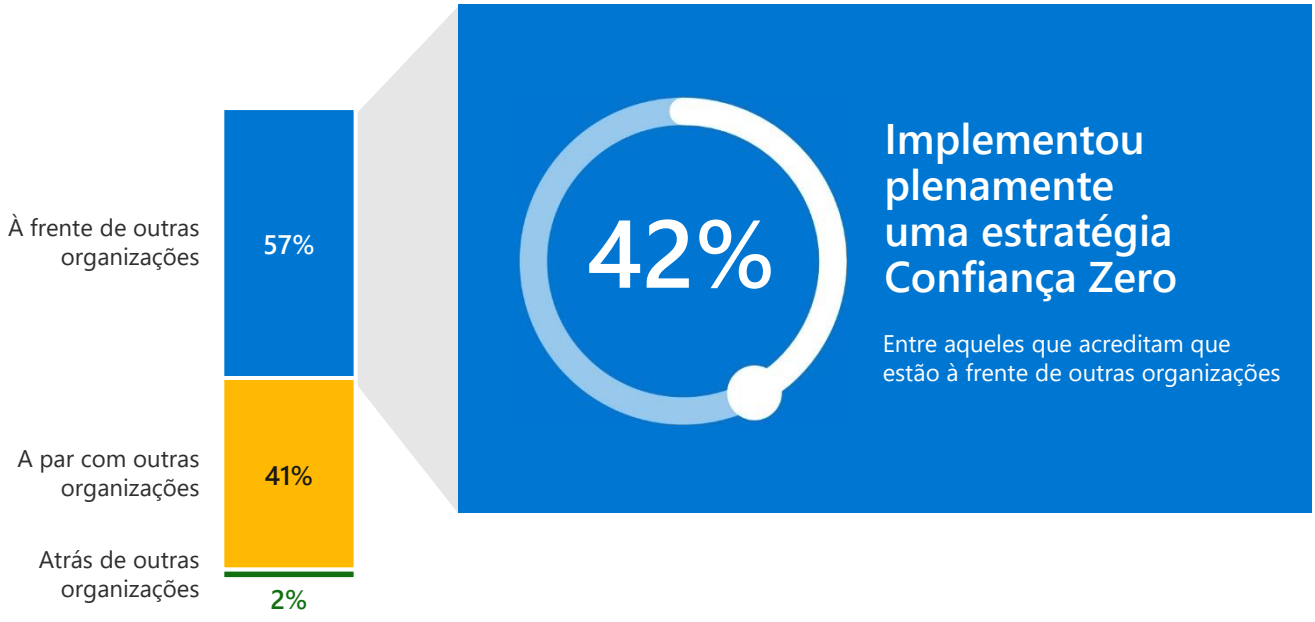
Tendo em conta os benefícios obtidos, a Confiança Zero geralmente reúne associações positivas. Nos quatro mercados, os SDM veem a abordagem das suas organizações como simultaneamente prática e aspiracional, descrevendo-a como confiante (37%) e eficiente (31%), bem como motivadora (25%), inspiradora (25%) e emocionante (25%). No Japão especificamente, os profissionais de segurança descrevem a Confiança Zero como exigente (27%) e transformacional (25%), sugerindo que, apesar de não ser fácil de implementar, os seus benefícios são de grande alcance uma vez adotados.

Muitos acreditam que estão à frente com a implementação da Confiança Zero, mas ainda têm mais a fazer

Embora apenas 35% das organizações tenham implementado plenamente a sua estratégia de Confiança Zero, 52% dizem que estão mais avançadas do que planeavam estar e 57% acreditam que estão à frente de outras organizações. As organizações consideram-se particularmente à frente de outras no Japão (66%) e na Austrália/Nova Zelândia (63%). Embora a confiança abunde nos mercados, parece haver um abismo entre perceção e realidade: entre aqueles que se sentem à frente de outras organizações, apenas 42% afirmam ter implementado plenamente uma estratégia de Confiança Zero. (Ver Anexo 9)

Embora muitas organizações estejam confiantes na sua estratégia de Confiança Zero e se sintam preparadas para lidar com futuras ameaças à segurança, há ainda muito trabalho a ser feito para implementar plenamente em todas as áreas de risco. Entre as organizações que consideram a sua estratégia de Confiança Zero totalmente implementada, por exemplo, quase metade ainda não implementou em áreas de risco de segurança, sendo as Infraestruturas e Identidades as menos prováveis de serem implementadas.

Anexo 9. Comparação de implementação Confiança Zero



	EUA	Alemanha	Japão	Austrália/ Nova Zelândia
À frente	59%	46%	66%	63%
A par	40%	52%	34%	32%
Atrás	2%	2%	0%	6%

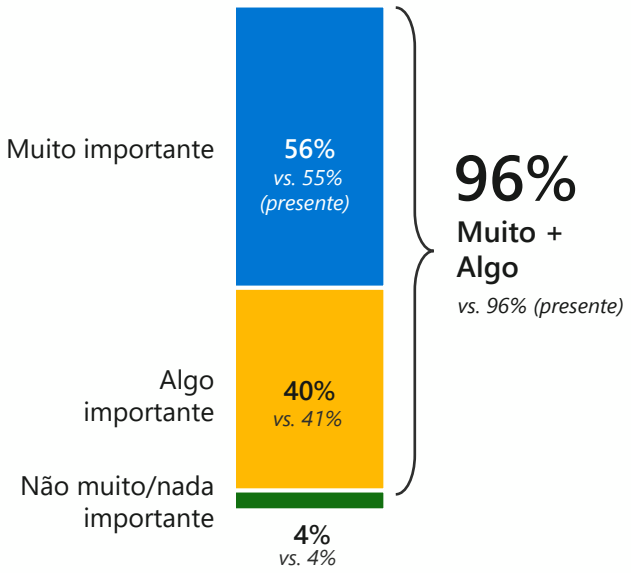
Microsoft Security hypothesis

Para os próximos dois anos, a estratégia de Confiança Zero continuará a ser uma prioridade máxima de segurança

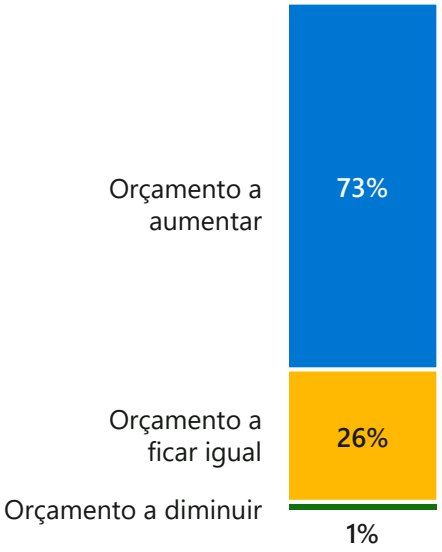
As organizações estão totalmente motivadas para a estratégia Confiança Zero, e os decision-makers dizem que continuará a ser a principal prioridade de segurança nos próximos dois anos. A importância relativa da estratégia de Confiança Zero como iniciativa de segurança deverá aumentar (53% a 58%) até 2023, uma vez que os SDM preveem que a estratégia continuará a ser fundamental para o sucesso global (96%). (Ver Anexo 10)

A importância crítica esperada é particularmente elevada entre as organizações japonesas, com 70% a afirmar que a estratégia de Confiança Zero será muito importante nos próximos dois anos, em comparação com a média geral de 56%. Espera-se também que os orçamentos da estratégia de Confiança Zero cresçam com 73% das organizações a esperarem aumentar os seus orçamentos. Embora este número seja ligeiramente inferior na Alemanha (67%), onde 31% antecipam que os seus orçamentos se mantenham iguais. (Ver Anexo 11)

Anexo 10. Importância antecipada da Confiança Zero nos próximos dois anos

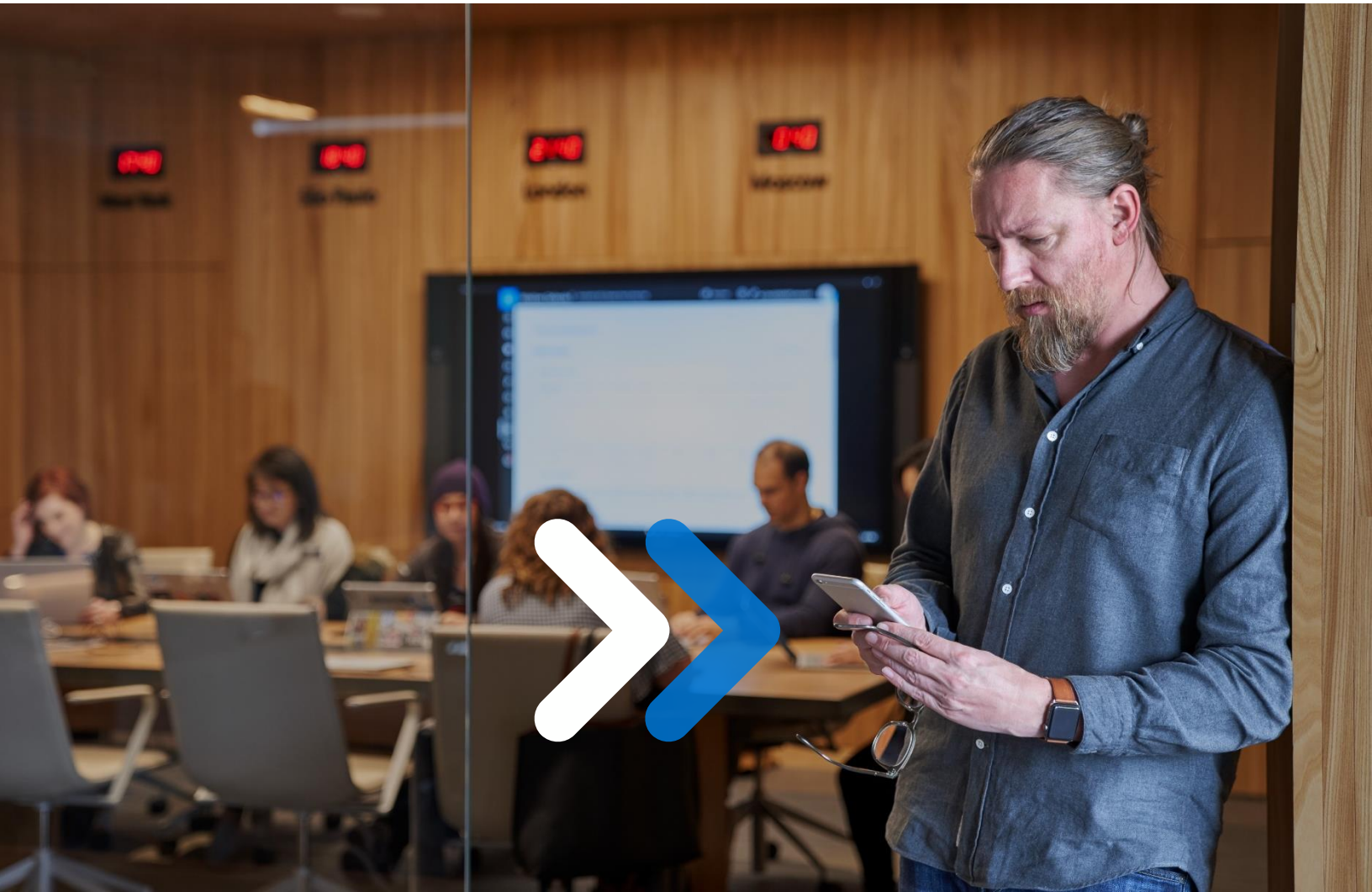


Anexo 11. Orçamento antecipado da Confiança Zero nos próximos dois anos



A comprovação do sucesso da estratégia da Confiança Zero poderia fomentar mais investimentos

As organizações que adotaram completamente a Confiança Zero esperam duplicar o seu investimento nos próximos dois anos, e aquelas que ainda não começaram a adotar arriscam ficar ainda mais para trás. Estas organizações não só seguem as suas homólogas totalmente implementadas quando se trata de dar prioridade à Confiança Zero nos seus planos de segurança (42% vs. 66%) e de antecipar aumentos orçamentais (66% vs. 72%), mas também se sentem significativamente menos confiantes na gestão da segurança da IoT e OT no futuro (40% vs. 53%).



Superar desafios com os colaboradores será a chave para duplicar o investimento da Confiança Zero

Apesar dos rápidos avanços na adoção da estratégia da Confiança Zero, as organizações têm de ultrapassar uma infinidade de desafios se quiserem avançar mais com a implementação. (Ver Anexo 12) Os desafios de recursos e liderança são mais predominantes nestas categorias. O tempo necessário para implementar as estratégias de Confiança Zero e a falta de apoio da liderança da direção encabeçam a lista de barreiras, sendo esta última particularmente notória na Austrália/Nova Zelândia (65%).

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

Por exemplo, 21% dos SDM citam dificuldades em provar o ROI de um investimento em Confiança Zero como um obstáculo à implementação, um desafio que pode levar a uma falta de entusiasmo da direção. Uma vez que os mercados não americanos têm mais probabilidades de ter restrições orçamentais (60% das organizações no Japão; 57% das organizações na Alemanha; 57% das organizações na Austrália/Nova Zelândia), é possível que isto tenha um efeito dominó, levando a uma implementação mais baixa e mais lenta das estratégias de Confiança Zero no Japão, Alemanha, e Austrália/Nova Zelândia, em comparação com os EUA.

Anexo 12. Barreiras à Confiança Zero

Desafios de Recursos 60%	Liderança 53%	Tecnológico 46%	Fornecedor 46%	Restrições Orçamentais 45%
20% demora muito tempo a implementar	**20%** Falta de apoio da liderança mais ampla da direção	**21%** Dificuldade em integrar soluções de segurança	**21%** Precisa de apoio de implementação dos fornecedores	**21%** Custo de implementação de uma estratégia Confiança Zero
19% Falta de gestão interna da mudança	**19%** Falta de apoio das partes interessadas	**19%** Incompatibilidade com sistemas legados	**21%** Dificuldade em identificar os fornecedores certos	**21%** dificuldade em provar o ROI
18% Precisa de mais materiais educativos	**19%** Precisa de ajuda para fazer um caso de negócio convincente	**19%** Dificuldade em escalar a toda a organização	**17%** Incapacidade de encontrar parceiros inovadores	**14%** Não tenho um orçamento suficientemente grande
17% Não é necessário para uma organização do nosso tamanho	**18%** Falta de buy-in organizacional			
16% Não tenho o talento certo para implementar corretamente				

"A adesão inicial foi um desafio, mas uma vez que concordámos como stakeholders que íamos investir neste projeto, todos estavam de acordo."

Security Decision-Maker dos EUA
FinTech

Os security decision-makers têm uma ligeira tendência para os prestadores holísticos ou consolidados

Quando se trata de estratégia de fornecedor de Confiança Zero, as organizações são confrontadas com a adoção de uma abordagem melhor fornecedor ou melhor software. A primeira estratégia envolve a compra de um conjunto de produtos para toda a arquitetura da Confiança Zero a um fornecedor holístico ou consolidado, uma solução que os SDM acreditam oferecer mais competências, recursos e simplicidade para aqueles que estão com os recursos internos limitados. No entanto, as preocupações com esta abordagem incluem uma maior vulnerabilidade e falta de flexibilidade. (Ver Anexo 13)

Esta última estratégia, o melhor software, envolve a obtenção de componentes tecnológicos individuais da Confiança Zero de fornecedores especializados. Ao contrário do melhor fornecedor, esta estratégia baseia-se em fornecedores especializados em diferentes áreas e, assim, oferecem maior flexibilidade e podem alinhar-se mais estreitamente com a estratégia da organização. Dito isto, os profissionais de segurança veem o melhor software como mais dispendioso, exigindo mais recursos, e inibindo a visibilidade, desvantagens que acabam por levar a desafios de fornecedor e orçamental. (Ver Anexo 14)

Embora as organizações estejam largamente divididas, uma ligeira maioria dos SDM (55%) prefere trabalhar com fornecedores holísticos (best-in-suite). (No entanto, as organizações na Austrália/Nova Zelândia inclinam-se na direção oposta, com 52% a preferirem o melhor software.)

Anexo 13. Benefícios e barreiras melhor fornecedor - Classificado no Top 2

⊕ Vantagens do melhor fornecedor	
O fornecedor tem conhecimentos específicos da indústria em soluções	24%
Mais recursos disponíveis para ajudar a planear a estratégia da Confiança Zero	23%
Stack de segurança simplificado	22%

⊖ Desvantagens do melhor fornecedor	
A dependência de um único fornecedor aumenta a vulnerabilidade	34%
Requer uma integração mais complexa com a arquitetura antiga	33%
Menor flexibilidade para o funcionamento especializado	29%

Anexo 14. Benefícios e barreiras melhor software - Classificado no Top 2

⊕ Vantagens do melhor software	
Flexibilidade para procurar as melhores soluções para qualquer componente da estratégia Confiança Zero	33%
Poder alinhar mais de perto a solução com a arquitetura ou estratégia da minha organização	30%
Maior oportunidade de inovação com vários fornecedores	26%

⊖ Desvantagens do melhor software	
Aumento dos custos	29%
Incapacidade de partilhar dados em diferentes soluções	26%
Elevado volume de soluções para as equipas internas adotarem e gerirem	26%

Reflexão final

À medida que os riscos de segurança se tornam não só mais frequentes mas também mais desastrosos, as organizações em todos os mercados e indústrias estão a optar por uma estratégia de Confiança Zero que nos guia para "nunca confiar, verificar sempre". A estratégia de Confiança Zero é a principal prioridade de segurança para organizações que visam melhorar a sua postura de segurança global, experiência do utilizador final e produtividade, simplificar os procedimentos de segurança para os colaboradores e reduzir os custos. Contudo, embora os benefícios de uma estratégia de Confiança Zero estejam bem estabelecidos, os recursos limitados e o ceticismo entre os líderes impedem a implementação universal.

A adoção da estratégia de Confiança Zero acelerou-se nos últimos três anos, em parte devido à pandemia da COVID-19. Particularmente, a mudança para locais de trabalho remotos e híbridos está a conduzir a uma maior adoção de abordagens de Confiança Zero, que prometem salvaguardar sistemas e dados mesmo quando os colaboradores acedem a eles fora do local, por vezes em dispositivos pessoais. A adoção acelerada devido à COVID é um bom preditor da prontidão da Confiança Zero em geral, tendo as organizações que abraçaram a estratégia durante a pandemia implementado em áreas de maior risco de segurança do que as suas homólogas.

Dito isto, mesmo os utilizadores mais avançados da estratégia de Confiança Zero têm ainda trabalho a fazer, e as incompreensões das organizações sobre a sua própria maturidade em termos de Confiança Zero podem deixar algumas com vulnerabilidades que nem sequer sabem que têm.

A maioria das organizações em todos os mercados acredita que a criticidade de uma estratégia de Confiança Zero só irá crescer com o tempo e espera que os seus orçamentos aumentem por sua vez. Esta mudança antecipada de prioridades é particularmente crucial para os mercados não-americanos, onde as preocupações orçamentais são obstáculos salientes à adoção. A luta pela plena implementação pode ser financeira e logisticamente devastadora; ainda assim, os benefícios de uma abordagem de Confiança Zero são inegáveis, e a Microsoft estará presente para orientar e apoiar as organizações à medida que estas embarcam nesta fronteira em expansão.

Para saber mais sobre Confiança Zero e fazer uma avaliação da maturidade da Confiança Zero da sua organização, visite

aka.ms/zerotrust

Objetivos de investigação detalhados e recrutamento de público

Os objetivos da investigação incluíam:

Entender o estado atual das abordagens da Confiança Zero

Descobrir mentalidades, melhores práticas, benefícios e desafios da adoção de abordagens de Confiança Zero

Explorar o futuro das abordagens Confiança Zero

Contextualizar inovações e tendências nas abordagens Confiança Zero

Para cumprir os critérios de seleção, os Security Decision-Makers precisavam de ser:

Responsáveis pela segurança na sua organização, incluindo Cibersegurança, Operações de Segurança, Proteção de Ameaças, Gestão de Identidade, Gestão de Riscos, Segurança de Aplicações, Forense Digital e Resposta a Incidentes

Empregado a tempo inteiro numa empresa (mais de 1000 colaboradores nos EUA; Mais de 500 colaboradores na Alemanha/ Japão/Austrália/Nova Zelândia)

Idades 25-75

Familiarizado com a Confiança Zero

Envolvido na tomada de decisões para desenvolvimento/implementação de estratégia Confiança Zero

Dos 911 Security Decision-Makers entrevistados para a vaga de investigação em abril de 2021:

Nos EUA, foram entrevistados 477 SDM

Na Alemanha, foram entrevistados 201 SDM

Na Austrália/Nova Zelândia, foram entrevistados 126 SDM

No Japão, foram entrevistados 107 SDM

Nota: a investigação foi realizada durante a pandemia global COVID-19, que se encontrava em diferentes fases de escalada/contenção

© Hypothesis Group 2021. © Microsoft 2021.
Todos os direitos reservados. 07/21

Microsoft Security hypothesis