O estado da transformação zero trust 2023

DA PREVENÇÃO À CAPACITAÇÃO:
aproveitando todo o potencial do zero trust para a empresa altamente móvel e centrada na nuvem

Índice

Resumo executivo

Nathan Howe | VP de Tecnologia Emergente e 5G da Zscaler

Em um cenário de rápida transformação digital, o zero trust surgiu como a estrutura ideal para proteger usuários, cargas de trabalho e dispositivos corporativos em um mundo altamente distribuído na nuvem e centrado na mobilidade.

Líderes de TI em todo o mundo estão percebendo isso, à medida que o zero trust se torna mais popular e rompe décadas de princípios de segurança e rede legados.

Mais de 90% dos líderes de TI que começaram a migrar para a nuvem implementaram ou estão no processo de implementar uma estratégia de segurança zero trust no próximo ano. Isso de acordo com as descobertas da nossa última pesquisa global, que colheu informações com mais de 1.900 CIOs, CISOs, CDOs e diretores de infraestrutura de empresas que já começaram a migrar seus aplicativos e serviços para a nuvem.

Este é um bom progresso, e as razões por trás dele demonstram um otimismo prolongado em implementar uma arquitetura zero trust para além dos próximos 12 meses.

22%

Com apenas 22% deles plenamente confiantes de que suas empresas estão aproveitando todo o potencial da infraestrutura na nuvem, os resultados indicam uma necessidade de, daqui para frente, considerar mais do que apenas a segurança

De fato, à medida que suas jornadas na nuvem avançam, os argumentos a favor do zero trust certamente parecem mais claros. Mais de dois terços (68%) dos líderes de TI concordam que a transformação segura na nuvem é impossível de implementar com a infraestrutura de segurança de rede legada ou que o acesso à rede zero trust tem vantagens óbvias em relação a firewalls e VPNs tradicionais, quando se trata de proteger o acesso remoto a aplicativos.

Mas com apenas 22% deles plenamente confiantes de que suas empresas estão aproveitando todo o potencial da infraestrutura na nuvem, os resultados indicam uma necessidade de, daqui para frente, considerar mais do que apenas a segurança. Quando visto a partir de uma perspectiva holística da TI, o zero trust tem o potencial de destravar uma série de oportunidades em um amplo processo de digitalização. Sim, ele pode evitar ataques de segurança cibernética em larga escala, mas também é capaz de fazer muito mais; desde promover mais inovação até apoiar um melhor engajamento dos funcionários ou fornecer eficiências de custos tangíveis.

À medida que as empresas lutam para oferecer uma nova classe de local de trabalho moderno — híbrido na abordagem e dependente de uma série de tecnologias emergentes, como IoT/TO, 5G e até mesmo do metaverso — elas devem ampliar o olhar pelo qual enxergam o zero trust e a transformação digital. Uma plataforma zero trust tem o poder de redefinir os requisitos comerciais e de infraestrutura organizacional: torna-se um verdadeiro promotor de negócios que não apenas permite que as empresas ofereçam o modelo de trabalho híbrido que os funcionários estão exigindo, mas também faz com que as empresas se tornem totalmente digitalizadas, com todos os benefícios que isso implica, desde agilidade e eficiência até uma infraestrutura preparada para o futuro.

Encomendamos essa pesquisa para descobrir o atual estado da transformação zero trust nas empresas. O que descobrimos é promissor — as taxas de implementação estão sólidas. Mas a lógica por trás da implementação poderia ser mais ambiciosa. Existe uma oportunidade incrível para que líderes de TI instruam os diretores de suas empresas sobre o modelo zero trust e o apresentem como um promotor de negócios de alto valor — atualmente, é o elo que faltava para ajudar as empresas a se capacitar e preparar para as tecnologias futuras.

ESTADO DO ZERO TRUST

90% Mais de 90% das empresas que começaram sua migração para a nuvem implementaram ou estão no processo de implementar uma estratégia de segurança zero trust nos próximos 12 meses

88% Em todo o mundo, 88% dos líderes de TI têm alguma confiança de que sua empresa está aproveitando o potencial da infraestrutura na nuvem, mas apenas 22% estão totalmente confiantes

REGIONALMENTE, OS NÍVEIS DE CONFIANÇA TOTAL NO APROVEITAMENTO DO POTENCIAL DA INFRAESTRUTURA NA NUVEM ESTÃO EM:

Nº 1 O ZTNA é a principal prioridade de investimento em tecnologia zero trust nos próximos 12 meses, o que mostra a importância do acesso remoto no ambiente de trabalho híbrido

68% Mais de dois terços (68%) dos líderes de TI concordam que é impossível realizar uma transformação segura na nuvem com uma infraestrutura de segurança de rede legada ou que o acesso à rede zero trust (ZTNA) tem vantagens óbvias em relação a firewalls e VPNs tradicionais, quando se trata de proteger o acesso remoto a aplicativos

54% dos líderes de TI indicaram acreditar que VPNs ou firewalls de perímetro são ineficientes na proteção contra ataques cibernéticos ou em oferecer visibilidade sobre o tráfego em aplicativos e ataques

AS PRINCIPAIS BARREIRAS IMPEDINDO O APROVEITAMENTO DE TODO O POTENCIAL DA NUVEM:

45% Desafios da proteção de dados na nuvem e preocupações sobre a privacidade dos dados

42% Complexidade da rede e dificuldade em dimensionar o hardware de segurança

40% Acesso remoto e de terceiros à IoT e TO

33% Conectividade inconsistente e experiência negativa de acesso remoto para os usuários

SEM CONSIDERAR SEGURANÇA, ACESSO E COMPLEXIDADE, AS PRINCIPAIS RAZÕES PARA IMPLEMENTAR UMA ARQUITETURA ZERO TRUST NÃO INCLUEM FATORES EMPRESARIAIS ESTRATÉGICOS:

65% Melhorar a detecção de ameaças avançadas ou de ataques a aplicativos web e ampliar a segurança de dados sigilosos

44% Proteger o acesso remoto de fornecedores, parceiros e tecnologia operacional

27% Melhorar a conectividade segura de uma força de trabalho híbrida

24% Reduzir os custos e a complexidade da segurança de rede legada

Seção I

O contexto da nuvem por trás da adoção do zero trust

Quando nos referimos à “nuvem” nesta pesquisa, estamos falando de aplicativos, dados e cargas de trabalho que são entregues como serviços hospedados na internet, em vez de um data center local em uma rede corporativa. Exemplos incluem Software como serviço (SaaS), Infraestrutura como serviço (IaaS), Plataforma como serviço (PaaS) ou aplicativos privados criados ou hospedados na nuvem.

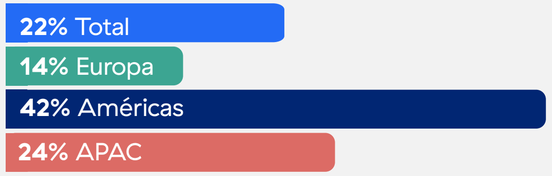
Antes de nos aprofundarmos nas peculiaridades do zero trust, gostaríamos de oferecer o contexto para sua adoção — examinar o que está acontecendo no panorama mais amplo de TI ao seu redor e, mais especificamente, ver onde as empresas estão atualmente em suas jornadas para a nuvem.

Não há dúvidas de que os eventos dos últimos anos aceleraram a migração para a nuvem. Em muitas empresas, o processo já está bastante avançado ou até mesmo concluído.

Entrevistamos mais de 1.900 CIOs, CISOs, CDOs, CTOs e diretores de infraestrutura ao redor do mundo, de empresas que já começaram a migrar seus aplicativos e serviços para a nuvem. Desses, quase metade (46%) afirmou que o processo de migração estava 100% concluído.

Mas embora 88% dos líderes de TI possuam algum nível de confiança de que estão aproveitando ao máximo sua jornada para a nuvem, apenas 22% estão plenamente confiantes de que sua empresa está utilizando todo o potencial da infraestrutura na nuvem atualmente.

ENTREVISTADOS MUITO CONFIANTES DE QUE SUA EMPRESA ESTÁ UTILIZANDO TODO O POTENCIAL DA INFRAESTRUTURA NA NUVEM ATUALMENTE



PORCENTAGEM DE ENTREVISTADOS MUITO CONFIANTES DE QUE SUA EMPRESA ESTÁ APROVEITANDO TODO O POTENCIAL DA INFRAESTRUTURA NA NUVEM ATUALMENTE

Passe o cursor sobre os países para ver mais detalhes.

Europa:

- 9% Alemanha
- 11% França
- 11% Espanha
- 19% Reino Unido

Américas:

- 41% EUA
- 51% Brasil

APAC:

- 16% Singapura
- 55% Índia

Examinando as diferenças regionais, os líderes de TI europeus demonstram ter mais dúvidas quanto ao uso da infraestrutura na nuvem, com apenas 14% expressando total confiança. Nas Américas, no entanto, esse número salta para 42%.

Embora não haja uma única causa para essa disparidade, uma possível razão pode ser as diferenças interculturais na velocidade de adoção de tecnologias inovadoras, pois a Europa tradicionalmente adota uma abordagem mais meticulosa e, além disso, dá mais ênfase à privacidade de dados. Além disso, com a já bem estabelecida infraestrutura de conectividade e o forte foco em fabricação da Europa, há um menor incentivo na adoção imediata de inovações como o 5G, e leva mais tempo para alterar os processos empresariais estabelecidos. Conforme será explorado em uma seção posterior, as empresas nas Américas dão mais ênfase a tecnologias emergentes, como inteligência artificial, aprendizado de máquina e realidade aumentada, o que sugere que já existem planos estabelecidos para que a infraestrutura na nuvem dê suporte a casos de uso mais sofisticados.

Mas, de forma mais ampla, por que as empresas estavam tendo dificuldade em desbloquear todo o potencial da nuvem?

Na superfície, a segurança aparece como a principal barreira, com os líderes de TI selecionando duas razões relacionadas à segurança como principal resposta à esta pergunta:

PRINCIPAIS BARREIRAS IMPEDINDO A ADOÇÃO DE TODO O POTENCIAL DA NUVEM

45% Preocupações sobre a privacidade dos dados e desafios em proteger os dados na nuvem

42% A adaptação de rede é altamente complexa e a segurança de rede é difícil de dimensionar

40% Desafios em habilitar o acesso de terceiros e o acesso remoto a sistemas de IoT e TO

33% Conectividade inconsistente e experiência negativa de acesso remoto para os usuários

AS PRINCIPAIS BARREIRAS IMPEDINDO A ADOÇÃO DE TODO O POTENCIAL DA NUVEM, POR PAÍS

Passe o cursor sobre os países para ver mais detalhes.

Em toda a região da Europa e APAC, as preocupações sobre privacidade de dados dominam:

- 36% Espanha
- 34% Índia
- 33% Itália
- 32% Austrália
- 28% França

Nas Américas, as empresas enfrentam desafios sobre a proteção de dados na nuvem:

- 44% Brasil
- 30% EUA

Enquanto isso, Singapura e Japão, em particular, estão com dificuldades em dimensionar o hardware de segurança de rede:

- 41% Singapura
- 30% Japão

Em um ambiente baseado na nuvem, a superfície de ataque aumenta exponencialmente, com cada serviço voltado à internet, usuário e dispositivo se tornando um possível ponto de entrada, uma porta principal que precisa ser protegida contra ameaças.

E as empresas têm bons motivos para se preocupar. Em um ambiente baseado na nuvem, a superfície de ataque aumenta exponencialmente, com cada serviço voltado à internet, usuário e dispositivo se tornando um possível ponto de entrada, uma porta principal que precisa ser protegida contra ameaças. Falaremos mais sobre isso em nossa próxima seção.

Mas basta olhar para as motivações gerais por trás das migrações para a nuvem para ver uma barreira muito mais fundamental sobre como os líderes de TI enxergam a nuvem — algo que sem dúvida está impactando seu uso efetivo. Quando perguntados sobre os principais fatores que estão promovendo a transformação digital em suas empresas, três deles se destacaram: reduzir custos, facilitar a inovação tecnológica e gerenciar o risco cibernético.

OS PRINCIPAIS FATORES QUE PROMOVEM OS PROJETOS DE TRANSFORMAÇÃO DIGITAL, DE ACORDO COM LÍDERES DE TI EM TODO O MUNDO, SÃO:

- Reduzir **custos de infraestrutura** de TI
- Facilitar inovações como **5G e computação de borda**
- Mitigar **riscos** de segurança cibernética
- Gerenciar **ambientes multinuvem**
- Melhorar a capacidade de atrair e reter os **melhores talentos**

OS PRINCIPAIS FATORES QUE PROMOVEM OS PROJETOS DE TRANSFORMAÇÃO DIGITAL, POR PAÍS

Passe o cursor sobre os países para ver mais detalhes.

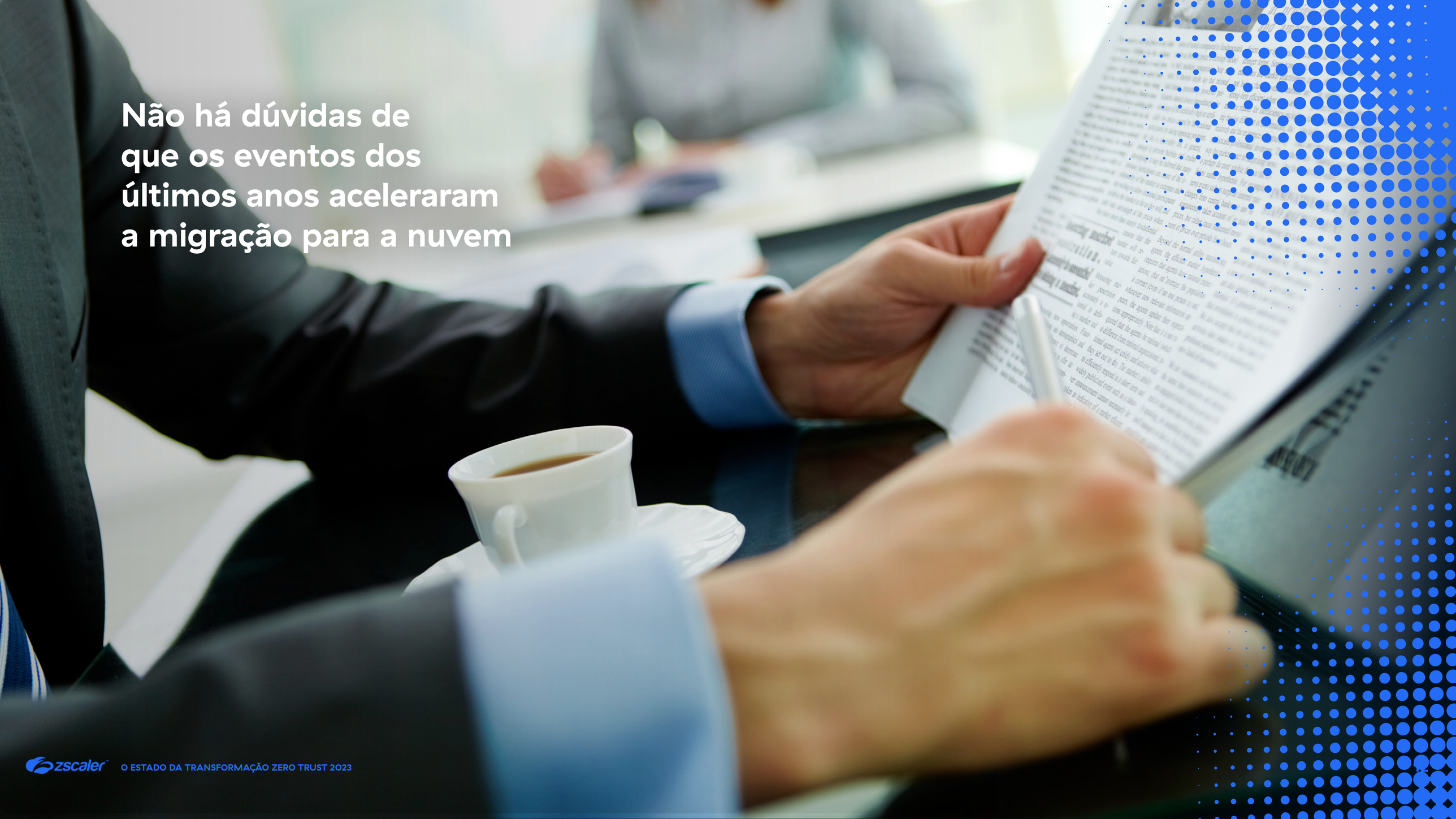
O Brasil se alinhou ao consenso global, com a maioria das empresas citando a redução de custos com infraestrutura de TI como o fator principal.

Em alguns países europeus, no entanto, não foi assim. Na França, as empresas estavam mais preocupadas em possibilitar o trabalho híbrido, enquanto a principal prioridade na Suécia era a experiência do usuário.

Facilitar inovações como o 5G e a computação de borda era mais importante em países mais voltados para o futuro, como Japão, México e Singapura. O crescimento de receita era igualmente importante em Singapura.

A otimização dos processos empresariais também ficou entre os três principais itens da lista no Brasil e na Espanha.

Tudo muito prático, e tudo promovido pela TI. Na verdade, a grande importância da redução de custos, embora compreensível no clima atual, indica que ainda pode haver uma nítida falta de compreensão sobre os principais benefícios da nuvem. E isso, por sua vez, pode estar afetando a abordagem e o uso dessas tecnologias que estão sendo trazidas para apoiá-la. **Entra em cena o zero trust.**



Não há dúvidas de que os eventos dos últimos anos aceleraram a migração para a nuvem

Seção II

Argumentos a favor do zero trust

O zero trust é uma abordagem holística para proteger empresas modernas, baseada no acesso de privilégio mínimo e no princípio de que nenhum usuário ou aplicativo deve ser inerentemente confiável. Esta abordagem pressupõe que tudo é hostil, e só estabelece uma relação de confiança com base na identidade do usuário e no contexto, com as políticas servindo de guardiãs o tempo todo. Nos Estados Unidos, o Instituto Nacional de Padrões e Tecnologia (NIST) define o princípio fundamental de uma arquitetura zero trust como: “nenhuma confiança implícita é concedida a ativos ou contas de usuário com base apenas em sua localização física ou de rede (por exemplo, redes de área local versus a internet) ou com base no proprietário dos ativos (de propriedade da empresa ou pessoal)”. É uma reformulação do antigo ditado: “Nunca confie. Sempre verifique.”

Com segurança, acesso e complexidade subindo para o topo da lista de preocupações sobre nuvem dos líderes de TI, não surpreende que mais empresas estejam vendo o zero trust como um meio de superar esses obstáculos. As respostas mostram que as empresas estão construindo uma boa base de compreensão sobre as vantagens de segurança do zero trust em comparação com abordagens mais tradicionais nesse novo ambiente operacional.

Quando perguntados sobre a infraestrutura de rede e segurança tradicionais, 54% dos líderes de TI indicaram acreditar que firewalls de perímetro ou VPNs são ineficientes na proteção contra ataques cibernéticos ou em oferecer visibilidade sobre o tráfego e os ataques sofridos por um aplicativo. Outros 68% reconheceram que, quando se trata de acesso remoto seguro a aplicativos, o acesso à rede zero trust (ZTNA) tem vantagens óbvias sobre firewalls e VPNs tradicionais ou que a transformação segura na nuvem não pode ser alcançada com uma infraestrutura de segurança de rede legada.

Passe o cursor sobre os países para ver mais detalhes.

Entrevistados que concordam que a transformação segura na nuvem é impossível de implementar com uma infraestrutura de segurança de rede legada e que o acesso à rede zero trust tem vantagens óbvias sobre os firewalls e VPNs tradicionais quando se trata de proteger o acesso remoto a aplicativos

- 85% Índia
- 81% EUA
- 75% Brasil
- 75% Singapura
- 73% Suécia

Entrevistados que concordam que VPNs / firewalls de perímetro não são eficazes na proteção contra ataques cibernéticos ou oferecem baixa visibilidade sobre o tráfego e os ataques sofridos por um dispositivo:

- 72% Índia
- 65% Singapura
- 64% Japão
- 57% Alemanha
- 56% EUA

Entrevistados que concordam que, além da segurança, as equipes de TI precisam de ferramentas integradas para analisar, solucionar e resolver com eficácia problemas de experiência de usuário:

- 70% Índia
- 63% México
- 62% EUA
- 56% Singapura
- 51% Espanha
- 50% Japão

90%

Mais de 90% dos entrevistados que começaram sua migração para a nuvem implementaram ou estão no processo de implementar uma estratégia de segurança zero trust nos próximos 12 meses.

Além da maior conscientização, o que demonstra ser mais promissor é que eles estão agindo de acordo. Mais de 90% dos entrevistados que começaram sua migração para a nuvem implementaram ou estão no processo de implementar uma estratégia de segurança zero trust nos próximos 12 meses.

A Itália e a Índia saltam à frente quando se trata de implementar uma estratégia de segurança zero trust, com 97% das empresas italianas e 96% das empresas indianas confirmando que já implementaram ou que estão implementando.

Passe o cursor sobre os países para ver mais detalhes.

Percentual de empresas que já implementaram a segurança zero trust, estão implementando-a ou estão no processo de planejamento estratégico para implementá-la:

- 97% Itália
- 96% Índia
- 95% Reino Unido
- 95% EUA
- 94% Japão
- 93% Brasil
- 93% Singapura
- 92% Alemanha
- 91% México
- 90% Países Baixos
- 89% Espanha
- 89% França
- 88% Austrália
- 85% Suécia

O zero trust ainda é visto predominantemente como uma solução (de segurança) isolada e centrada na TI... mas o zero trust pode oferecer muito mais do que isso às empresas.

Mas, infelizmente, implementar um sistema de segurança zero trust ou ter planos para implementá-lo certamente não indica que ele está sendo aproveitado ao máximo como um capacitador de negócios.

Na verdade, as descobertas indicam que o zero trust ainda é visto predominantemente como uma solução (de segurança) isolada e centrada na TI, o que significa que os desafios de segurança imediatos estão sendo resolvidos e os benefícios táticos estão sendo alcançados — mas o zero trust é capaz de oferecer muito mais do que isso às empresas.

PRINCIPAIS RAZÕES PARA IMPLEMENTAR UMA ARQUITETURA ZERO TRUST

65% Melhorar a detecção de ameaças avançadas ou de ataques a aplicativos web e ampliar a segurança de dados sigilosos

44% Proteger o acesso remoto de fornecedores, parceiros e tecnologia operacional

27% Melhorar a conectividade segura de uma força de trabalho híbrida

24% Reduzir os custos e a complexidade da segurança de rede legada

PRINCIPAL RAZÃO PARA IMPLEMENTAR UMA INFRAESTRUTURA ZERO TRUST AO REDOR DO MUNDO:

Passe o cursor sobre os países para ver mais detalhes.

Melhorar a detecção de ameaças avançadas:

- 52% Índia
- 42% Singapura
- 41% EUA
- 39% Itália
- 35% Espanha
- 30% França
- 26% Reino Unido

Melhorar a detecção de ataques a aplicativos web:

- 44% Brasil
- 35% México

Ampliar a segurança para proteger dados sigilosos:

- 44% Brasil

Oferecer acesso remoto seguro para fornecedores, parceiros e prestadores de serviço:

- 33% Austrália
- 32% Japão
- 24% Países Baixos

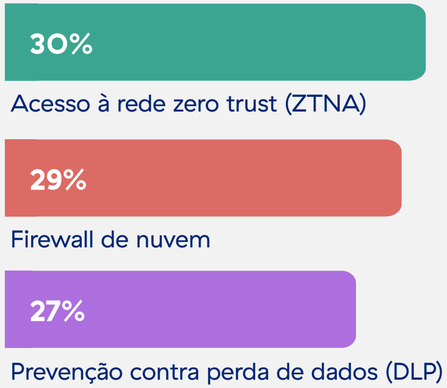
Essa abordagem ao zero trust, de usá–lo para fins de segurança somente no começo da jornada de transformação, limita consideravelmente o seu potencial de velocidade e dimensionamento, em um momento que depende muito da capacidade de uma empresa se digitalizar e inovar.

Quando corretamente compreendido e não visto meramente como uma tecnologia ou produto, ele permite que as empresas simplifiquem sua infraestrutura e repensem o modo de fazer negócios, além de permitir que a empresa se transforme em um negócio totalmente digitalizado. Por exemplo, as empresas que alcançaram o modelo zero trust possuem um inventário completo e preciso de todos os seus aplicativos e de tudo que possuem dentro da empresa. Com base nesse inventário, elas conseguem tomar decisões estratégicas sobre como otimizar processos, reduzir custos, eliminar o hardware legado e melhorar a eficiência.

Mas para alcançar esses benefícios estratégicos, a mensagem do zero trust deve ser capaz de entrar na sala de reuniões e se tornar parte da estratégia geral da empresa. Hoje, está claro que ainda há incerteza e, provavelmente, falta de conhecimento prático sobre o que o zero trust significa e quais são seus impactos nos negócios. A tarefa primordial em mãos é ajudar líderes empresariais, incluindo CIOs, a entender que o objetivo do zero trust é introduzir simplicidade na infraestrutura geral, removendo hardwares que exigem muita administração para oferecer, com mais facilidade, os resultados comerciais exatos que uma empresa precisa — e manter uma segurança de alto nível ao mesmo tempo.

Olhando para as tecnologias zero trust que as empresas estão priorizando nos investimentos dos próximos doze meses, vê–se algumas evidências de que esse entendimento dos benefícios comerciais está evoluindo, ainda que a ritmos bem distintos em diferentes regiões do mundo, e com ampla margem para melhorias.

PRINCIPAIS TECNOLOGIAS ZERO TRUST EM QUE AS EMPRESAS ESTÃO INVESTINDO



PONTO DE VISTA REGIONAL: A VOZ DAS AMÉRICAS

Amit Chaudhry, Diretor Sênior, Marketing de Produto

Atualmente, as empresas estão adotando as tecnologias de nuvem, mobilidade, IA, IoT e TO para tornar os negócios mais ágeis e competitivos. Os usuários estão em todos os lugares, assim como seus dados. Mas, naturalmente, para obter uma colaboração rápida e produtiva, eles querem acesso direto aos aplicativos de qualquer lugar e a qualquer hora.

Esse ritmo explosivo de transformação digital proporcionou aos criminosos uma janela de oportunidade para explorar arquiteturas de rede e segurança com décadas de existência. A quantidade de ataques cresceu exponencialmente, em particular os ataques de ransomware e de cadeia de suprimentos. E à medida em que esses ataques se tornam mais sofisticados, a segurança baseada em perímetro que utiliza VPNs e firewalls não consegue mais proteger a rede e fornecer uma boa experiência aos usuários.

Para concretizar a visão de um espaço de trabalho híbrido seguro, as empresas estão rapidamente se afastando dos firewalls e VPNs e indo em direção à arquitetura zero trust, que protege o acesso rápido e direto a aplicativos, de qualquer lugar e a qualquer hora. Desenvolvido sobre o princípio do acesso de privilégio mínimo, onde a conexão é feita com base na identidade e no contexto, o zero trust talvez seja a ideia mais simples e mais importante sobre a forma como os dados são protegidos.

Hoje, está claro que ainda há incerteza e, provavelmente, falta de conhecimento prático sobre o que o zero trust significa e quais são seus impactos nos negócios

Seção III

Recorrendo ao zero trust para oferecer opções de trabalho híbrido

A infraestrutura de trabalho híbrido se refere a uma infraestrutura que permite que os funcionários alternem sem problemas entre ambientes de trabalho de locais físicos e remotos, sem qualquer limitação ou complexidade administrativa.

Quando os primeiros lockdowns fizeram com que as empresas tivessem dificuldade em acomodar seus funcionários para trabalhar de casa, mal sabíamos que essa "medida temporária" abriria as portas para uma maneira totalmente nova de trabalhar e que, de fato, o próprio trabalho nunca mais seria o mesmo.

Atualmente, a força de trabalho tem opções: trabalhar de casa, do escritório ou de qualquer outro local — e eles têm (ou deveriam ter) a tecnologia para fazer isso acontecer.

Os entrevistados previram que nos próximos 12 meses, sua força de trabalho ainda estará adotando plenamente as diferentes opções disponíveis, dividida entre trabalho presencial em tempo integral (38%), trabalho totalmente remoto (35%) e trabalho híbrido (27%).

Esses números permanecem relativamente consistentes ao redor do mundo.

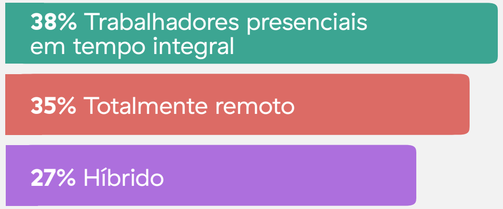
Embora quase dois terços (62%) dos líderes de TI digam que suas empresas adotam o trabalho híbrido ou oferecem à sua equipe flexibilidade total para trabalhar remotamente, o fato de mais de um terço (38%) prever que voltará para o escritório em tempo integral é surpreendente e preocupante.

Embora isso possa ser compreensível para certos setores que dependem de interações presenciais (como saúde e hotelaria), em condições favoráveis de mercado isso também poderia levar muitas empresas a ter dificuldade em atrair e reter talentos, pois não poderiam oferecer o ambiente de trabalho flexível com o qual os funcionários se acostumaram nos últimos anos.

19%

Em todo o mundo, apenas 19% dos tomadores de decisões de TI entrevistados indicaram ter uma infraestrutura baseada em zero trust específica para a força de trabalho híbrida já ativa.

PERCENTUAL DA FORÇA DE TRABALHO TOTALMENTE REMOTA, TOTALMENTE PRESENCIAL OU HÍBRIDA QUE SE ESPERA TER NOS PRÓXIMOS 12 MESES



Intenções à parte, a sua infraestrutura de TI e segurança estar totalmente equipada para lidar com essa combinação em evolução é uma questão completamente diferente. Em todo o mundo, apenas 19% dos tomadores de decisões de TI entrevistados indicaram ter uma infraestrutura específica baseada em zero trust para a força de trabalho híbrida já ativa, o que mostra que as empresas ainda não estão totalmente prontas para lidar com esse ambiente de trabalho altamente distribuído em larga escala. Ao lado dos que já atualizaram sua infraestrutura, outros 50% estão no processo de implementação ou planejando uma estratégia híbrida baseada em zero trust.

E entre aqueles que estão implementando ou planejando implementar o zero trust para oferecer acesso remoto seguro a fornecedores, parceiros, prestadores de serviço ou operadores de equipamentos e fábricas — ou seja, aqueles que por padrão já trabalham em um ambiente híbrido — há um claro indicador de que o acesso à rede zero trust é uma área prioritária de investimento nos próximos 12 meses. Isso sugere haver uma alta demanda para atender aos desafios imediatos da mudança em curso para um cenário de trabalho híbrido.

Passe o cursor sobre os países para ver mais detalhes.

Implementar uma estratégia híbrida baseada em zero trust é prioridade em:

- 37% Índia
- 36% Singapura
- 33% Japão
- 29% Alemanha
- 29% Países Baixos

Enquanto isso, os seguintes países ainda estão predominantemente na etapa de planejamento:

- 34% México
- 27% EUA
- 27% França
- 25% Suécia

Em geral, o Reino Unido parece ser a nação mais relutante em adotar estratégias híbridas baseadas no zero trust, com 21% das empresas dizendo que atualmente não possuem planos de implementar uma infraestrutura híbrida, e outros 20% preferindo permanecer com suas tecnologias de acesso remoto tradicionais.

Naturalmente, a segurança é uma das principais preocupações de empresas cada vez mais híbridas.

PRINCIPAIS PREOCUPAÇÕES DE SEGURANÇA EM EMPRESAS MIGRANDO PARA O TRABALHO HÍBRIDO:

- **54%** sistemas de tecnologia operacional (TO) e acesso à internet
- **53%** Aplicativos privados no local ou aplicativos privados e cargas de trabalho na nuvem (em IaaS, PaaS)
- **32%** Internet das coisas e acesso remoto à internet

Mas é importante notar que esses resultados mostram que a segurança em um ambiente de trabalho híbrido não se trata apenas de manter as ameaças afastadas — trata-se também de oferecer acesso à infraestrutura de forma segura para uma ampla gama de usuários, desde funcionários a fornecedores terceirizados e parceiros comerciais.

Com base nisso, apesar do compreensível foco em segurança, as razões oferecidas por aqueles que estão implementando ou planejando implementar uma infraestrutura de trabalho híbrida baseada em zero trust também começam a se referir aos impactos comerciais mais amplos das soluções de zero trust, com implicações sobre a experiência e produtividade dos funcionários.

RAZÕES PARA IMPLEMENTAR OU PLANEJAR A IMPLEMENTAÇÃO DE UMA INFRAESTRUTURA DE TRABALHO HÍBRIDA BASEADA EM ZERO TRUST

- **52%** Os funcionários enfrentam experiências de acesso inconsistentes para aplicativos e dados no local ou baseados na nuvem
- **46%** Os funcionários enfrentam perda de produtividade devido a problemas de acesso à rede
- **39%** Os funcionários não conseguem acessar aplicativos e dados a partir de dispositivos pessoais

Passe o cursor sobre os países para ver mais detalhes.

Os países que mais relataram ter experiências de acesso inconsistente foram

- 70% Japão
- 68% Índia
- 64% EUA
- 62% Singapura

Na Europa, cerca de metade das empresas entrevistadas relataram sofrer da mesma inconsistência, com

- 52% Suécia
- 49% Países Baixos
- 47% França
- 45% Alemanha

Perda de produtividade devido a problemas de acesso à rede foi citada como a principal razão para mudar para uma nova infraestrutura em

- 55% México
- 48% Espanha
- 47% Reino Unido

Os entrevistados cujas empresas utilizam infraestruturas de trabalho remoto tradicionais baseadas em VPN relataram ainda ter dificuldades com alguns problemas mais fundamentais do trabalho remoto.

A experiência do usuário é vital para a produtividade em ambientes de trabalho híbridos — esse é um dos principais aprendizados do último ano. E nossos resultados indicam que, até o momento, as regiões reagiram com velocidades diferentes no que tange a modernização da infraestrutura para solucionar os problemas de experiência.

Para oferecer ótimas experiências aos usuários no atual ambiente corporativo cada vez mais disperso, o tráfego de usuários deve ser direcionado ao aplicativo pela rota mais curta possível para evitar problemas de latência e congestionamento. As empresas devem considerar a mobilidade do funcionário híbrido moderno, que deve ser roteado dinamicamente para o aplicativo necessário de qualquer local com largura de banda otimizada, seja trabalhando de casa, no escritório ou em trânsito. Experiência à parte, se um funcionário estiver insatisfeito com o desempenho do acesso aos seus aplicativos comerciais de uso essencial, ele também poderá buscar maneiras de evitar os controles de segurança, aumentando ainda mais o potencial de impactos negativos.

Em comparação, os entrevistados cujas empresas utilizam infraestruturas de trabalho remoto tradicionais baseadas em VPN relataram ainda ter dificuldades com alguns problemas mais fundamentais do trabalho remoto. Entre eles, a complexidade em administrar diferentes infraestruturas de segurança para funcionários presenciais e remotos (47%), o baixo desempenho de aplicativos (39%) e a dificuldade da TI em monitorar e solucionar problemas de experiência dos usuários remotos (37%).

Embora ainda existam muitas preocupações de segurança sobre a migração para o trabalho híbrido, respostas como essas refletem o desafio muito maior que as formas de trabalho híbrido apresentam às empresas — um desafio que engloba o acesso, a experiência e o desempenho.

O zero trust, quando compreendido corretamente, oferece uma resposta a todos esses problemas, proporcionando uma simplicidade que permite à TI focar sua atenção em reagir às expectativas e exigências comerciais em constante mudança.

PONTO DE VISTA REGIONAL: A VOZ DA APAC

Heng Mok, CISO, APJ

A região Ásia–Pacífico (APAC) é um ótimo exemplo de como "não existe uma solução universal". Por ser um caldeirão de diferentes culturas e estilos de vida, cada mercado nessa região tem uma abordagem diferente ao trabalho. Mesmo antes da pandemia, observamos diferenças significativas, com mercados como Japão e Singapura seguindo uma estrutura mais hierárquica, enquanto Austrália e Índia tinham um modelo de trabalho mais descontraído.

Com a região da APAC incluindo algumas das cidades que mais impuseram restrições em todo o mundo, essas nuances se tornaram ainda mais evidentes agora, à medida em que saímos dos lockdowns. Entre os entrevistados, a maioria dos tomadores de decisões de TI do Japão e Singapura esperava que sua força de trabalho trabalhasse presencialmente em tempo integral, em contraste gritante com os entrevistados da Austrália e Índia, que esperavam que sua força de trabalho fosse totalmente remota.

No entanto, esperamos ver ainda mais empresas apostando em modelos de trabalho híbrido no longo prazo. Muitas empresas com as quais conversei estão optando por adotar práticas de trabalho híbrido para colher os benefícios intangíveis de atrair e reter talentos. Com a competição acirrada e um banco de talentos limitado, não surpreende que muitas delas estejam incorporando políticas similares e recorrendo a pilhas de tecnologia para dar suporte a esta transição de forma muito mais harmoniosa.

A experiência do usuário é vital para a produtividade em ambientes de trabalho híbridos — esse é um dos principais aprendizados do último ano.

Seção IV

Adotando uma abordagem zero trust para integrar tecnologias emergentes

Tecnologias emergentes são tecnologias novas ou em rápido desenvolvimento, cujas aplicações práticas em grande parte ainda não se concretizaram, mas a expectativa é que tenham um impacto significativo nos negócios e gerem vantagem competitiva.

É claro que as soluções digitais que permitem o trabalho remoto não são as únicas tecnologias que as empresas estão tentando adquirir. Na era digital atual, a tecnologia operacional desempenha um papel cada vez maior. Esse segmento do modelo de negócios de uma empresa, que historicamente tem se baseado fortemente em sistemas e processos legados, verá uma mudança transformadora fundamental em direção a novas tecnologias emergentes, cada qual com seu próprio conjunto de possibilidades interessantes para simplificar e automatizar ainda mais os processos empresariais.

Mas as empresas precisam pensar ainda mais à frente, levando também em consideração os próximos avanços tecnológicos para tomar decisões sobre infraestrutura já preparadas para o futuro. Os tomadores de decisões de TI precisam assumir a responsabilidade sobre as várias direções que a empresa pode tomar, com base em inovações, e ter a mente aberta sobre como as tecnologias emergentes podem dar suporte às funções comerciais de maneira eficaz. O zero trust pode ser o elo que falta para ajudar as empresas a aproveitar e a se preparar para tecnologias futuras, agora.

De acordo com as motivações por trás da migração para a nuvem e a transformação digital em geral, nossos resultados mostraram que um foco em resultados estratégicos mais amplos é algo que parece estar faltando na forma como as empresas estão planejando seus projetos de tecnologias emergentes.

Quando perguntados sobre qual é o aspecto mais desafiador na implementação de projetos de tecnologias emergentes, 30% disseram segurança adequada, seguido por requisitos orçamentários para digitalização adicional (23%). No entanto, apenas 19% citaram a dependência em decisões comerciais estratégicas como um desafio.

O ASPECTO MAIS DESAFIADOR NA IMPLANTAÇÃO DE PROJETOS DE TECNOLOGIAS EMERGENTES, POR REGIÃO

Passe o cursor sobre os países para ver mais detalhes.

As preocupações com segurança representaram o maior desafio para os seguintes países

- 54% Brasil
- 41% Japão
- 37% Índia
- 37% Itália
- 35% Espanha
- 31% EUA

Enquanto isso, os seguintes países têm dificuldades principalmente com as exigências orçamentárias:

- 27% Singapura
- 27% França
- 23% Reino Unido

A falta de visão parece ser o principal obstáculo entre as empresas e as tecnologias emergentes

- 24% Países Baixos

O único país onde a maior parte das empresas identificou uma dependência em decisões comerciais estratégicas como o maior obstáculo

- 28% Suécia

Embora as preocupações com orçamento sejam previsíveis, é interessante notar o foco na proteção de rede sem considerar o alinhamento estratégico comercial. As empresas estão focadas na segurança sem compreender totalmente seus benefícios comerciais — o que comprova mais uma vez que o zero trust ainda não é visto como um facilitador de negócios.

À medida em que elas se planejam para casos de uso de tecnologias emergentes, como realidade aumentada, gêmeos digitais e construção virtual, o acesso a aplicativos com baixa latência e alto desempenho também se torna uma preocupação. Esse é especialmente o caso das Américas, onde o interesse em tecnologias emergentes para os próximos três anos também é bastante alto.

RELEVÂNCIA DO ACESSO A APLICATIVOS COM BAIXA LATÊNCIA E ALTO DESEMPENHO NOS PRÓXIMOS TRÊS ANOS

TECNOLOGIAS DE MAIOR PRIORIDADE ATÉ 2025	GLOBAL	EUROPA	AMÉRICAS	APAC
Acesso baseado na nuvem a sistemas de tecnologia operacional e controle industrial	34%	29%	40%	38%
Implementação de tecnologia 5G para maior conectividade	32%	29%	39%	32%
Redução da pegada de carbono da empresa	29%	28%	28%	30%
Implementação de projetos de inteligência artificial/ aprendizado de máquina	27%	22%	39%	28%

Passe o cursor sobre os países para ver mais detalhes.

Empresas que estão focando no acesso baseado na nuvem para TO e controle industrial:

- 46% México
- 45% Índia
- 44% Singapura
- 36% Austrália
- 33% França

Empresas que estão priorizando a implementação de tecnologias 5G:

- 47% Brasil
- 45% Índia
- 41% Itália
- 36% Espanha
- 28% Reino Unido

Empresas que afirmam que a redução da pegada de carbono é sua prioridade nº 1:

- 41% Itália
- 28% Alemanha
- 32% Suécia

Apenas empresas nos Países Baixos veem a expansão da computação de borda como mais importante (29%), enquanto os EUA estão fortemente focados na implementação de projetos de IA e ML (43%).

Já podemos começar a ver como essas tecnologias emergentes priorizadas poderiam proporcionar resultados comerciais mais amplos. No entanto, nossos resultados ainda sugerem que falta uma visão mais ampla às empresas. É preciso haver um alinhamento muito mais consciente nas empresas sobre as vantagens competitivas que podem ser obtidas através das tecnologias emergentes e sua implantação estratégica — o que também inclui como elas são protegidas.

PONTO DE VISTA REGIONAL: A VOZ DA EMEA

Nathan Howe, VP de Tecnologias Emergentes

As empresas europeias são menos propensas a serem pioneiras na adoção de tecnologias novas ou emergentes. Mesmo que a Europa tenha sido o berço da revolução industrial com as invenções mecânicas, a região foi ultrapassada há muito tempo em relação à adoção de tecnologias digitais. A APJ se tornou o centro de gravidade para tecnologias de fabricação de chips, e o conhecimento para inovar une pessoas de todo o mundo para desenvolver tecnologias transformadoras no Vale do Silício.

Nesse contexto, não surpreende que a Ásia já tenha reconhecido o poder do 5G para além das redes sem fio, em uma próxima forma de conectividade como base para a digitalização. Enquanto as Américas estão no meio do caminho, a Europa ainda não tem certeza de como se atualizar para o 5G em seus esforços de digitalização. No entanto, a Europa está pronta para crescer drasticamente com relação à nuvem digital e em tecnologias emergentes, à medida que as mudanças de tendências geopolíticas, como falta de chips e problemas da cadeia de suprimentos, exigem que os países estabeleçam centros de excelência na região.

Seção V

O caminho para desbloquear todo o potencial do zero trust

Com base nessas descobertas, como as empresas devem abordar suas jornadas zero trust?

Os desafios trazidos pelas arquiteturas de rede e segurança legadas são generalizados, prolongados e exigem uma reflexão sobre como a conectividade é concedida no mundo moderno. É aqui que a arquitetura zero trust deve ser aproveitada — uma arquitetura onde nenhum usuário ou aplicativo é considerado confiável por padrão. O zero trust se baseia no acesso de privilégio mínimo, garantindo que a confiança seja concedida somente quando a identidade e o contexto forem confirmados e as verificações de políticas forem aplicadas.

Essa abordagem trata todas as comunicações de rede como hostis, e as comunicações entre usuários e cargas de trabalho ou entre as próprias cargas de trabalho são bloqueadas até que sejam validadas por políticas baseadas na identidade. Isso garante que o acesso inapropriado e a movimentação lateral sejam evitados. Essa validação se expande a qualquer ambiente de rede, e o local de rede de uma entidade não é mais um fator e não depende de uma segmentação rígida da rede.

O zero trust nasceu como uma nova maneira de proteger redes. Eventualmente, ele se expandiu para além das redes locais, mas ainda era voltado principalmente à proteção do tráfego de aplicativos privados. Durante muito tempo, o tráfego foi considerado com base em sua relação à uma rede, em vez de eliminar a rede por completo. Hoje, as empresas precisam se conscientizar sobre todo o potencial do zero trust na proteção de aplicativos SaaS, tráfego de entrada e saída de nuvens públicas e até mesmo de usuários que acessam a internet pública. E os originadores desse tráfego podem ser cargas de trabalho e também usuários. O acesso pode ser feito independentemente do meio de transporte, com o tráfego fluindo por qualquer roteador e passando por qualquer rede, com ou sem fio, 4G ou 5G, e futuras extensões.

Já passou da hora de aplicar os princípios do modelo zero trust a todo o tráfego, não importando sua origem ou destino. É hora de parar de pensar sobre qual entidade está se conectando a qual rede e usar o zero trust para conectar todas as entidades de forma direta usando políticas corporativas. Na era da nuvem, a internet é a nova rede corporativa, e todo tráfego é válido para conectar a entidade certa ao ativo certo diretamente utilizando políticas comerciais.

Quais medidas as empresas podem começar a tomar hoje mesmo para garantir que possam se transformar nas empresas seguras, ágeis, flexíveis e eficientes que precisam ser para lidar não apenas com os ambientes macroeconômicos atuais, mas também com as exigências das tecnologias emergentes?

Existem três recomendações principais:

1

As empresas precisam reconsiderar seu entendimento do zero trust, vendo ele como um capacitador da transformação digital segura e um promotor de resultados comerciais

Com os níveis crescentes de visibilidade e controle, uma arquitetura baseada em zero trust remove a complexidade da TI moderna e permite que as empresas se concentrem em obter os resultados que precisam de suas tecnologias, desde alto desempenho e melhor experiência do usuário até redução de custos.

2

É necessário instruir mais para dissipar o medo, a incerteza e as dúvidas sobre o que significa o zero trust e todo o impacto que ele tem nos negócios

O CIO e o CISO possuem um papel vital a desempenhar para fazer a mensagem ampla do zero trust chegar à diretoria, mostrando como ele se alinha à estratégia comercial.

3

As tecnologias emergentes precisam ser vistas como uma vantagem comercial competitiva, e atualmente infraestruturas habilitadas para o zero trust estabelecem a base para o futuro

A decisão de quais tecnologias emergentes buscar deve ser conduzida pela visão geral do negócio e pelas necessidades atuais e futuras da empresa, não por tendências ou por ser “legal”. O zero trust está aqui para auxiliar os requisitos de conectividade segura e eficiente das tendências emergentes.

Então, assim que a mentalidade tiver mudado para reconhecer que o zero trust é um verdadeiro capacitador de negócios, como as empresas devem agir para garantir uma arquitetura zero trust que seja bem sucedida em alcançar esses resultados comerciais?

A Zscaler implementou o modelo zero trust como um componente arquitetônico central da plataforma Zero Trust Exchange, e ele permeia cada elemento da estrutura de SSE. Isso inclui uma abordagem zero trust para usuários que acessam qualquer aplicativo (interno ou externo), conectividade IoT/TO e cargas de trabalho que acessam recursos em um ambiente multinuvem ou na própria internet. Os princípios do zero trust permitem utilizar o trabalho híbrido seguro de qualquer lugar como uma estratégia comercial, permitindo que funcionários, parceiros comerciais e clientes trabalhem do local mais adequado à sua produtividade — uma necessidade fundamental para a continuidade dos negócios, a aquisição de talentos remotos e o fornecimento de ambientes de trabalho híbrido cada vez mais populares.

A Zscaler Zero Trust Exchange é um serviço nativo da nuvem que oferece a funcionários, parceiros e clientes acesso rápido, direto e seguro a aplicativos internos e externos, independentemente de local, dispositivo ou rede.

O serviço também incorpora os sete elementos essenciais da arquitetura zero trust, que estão agrupados nas três categorias seguintes:

Verificar

A arquitetura zero trust primeiro encerra a conexão e determina

1. Quem está se conectando?
2. Qual é o contexto de acesso?
3. Para onde vai a conexão?

Controlar

A arquitetura zero trust tem como objetivo:

4. Avaliar os riscos
5. Evitar comprometimentos
6. Prevenir contra perda de dados

Aplicar

Antes de finalmente estabelecer uma conexão, a arquitetura zero trust vai:

7. Aplicar políticas

Ter esses elementos em mente será a base para que empresas que priorizam a nuvem acelerem a transformação digital e tornem-se empresas preparadas para o que vier no futuro.

Sobre a Zscaler e a Zscaler Zero Trust Exchange

A Zscaler é mundialmente reconhecida como líder em zero trust, com a maior, mais fácil de usar e mais madura plataforma de zero trust.

Você pode contar com a Zscaler Zero Trust Exchange, nossa plataforma nativa da nuvem, na sua jornada zero trust. Ao contrário dos produtos de rede e segurança legados, a Zero Trust Exchange é uma plataforma de nuvem criada sob medida. Sua segurança começa com o encerramento de cada conexão, o que permite fazer uma inspeção profunda do conteúdo e a verificação dos direitos de acesso com base na identidade e no contexto.

A Zero Trust Exchange opera em 150 data centers ao redor do mundo, garantindo que o serviço esteja próximo de seus usuários, em espaços compartilhados com os provedores de nuvens e os aplicativos sendo acessados, como Microsoft 365 e AWS. A plataforma garante o caminho mais curto entre os usuários e seus destinos, oferecendo segurança abrangente e uma incrível experiência ao usuário.

Saiba mais sobre a nossa plataforma fácil de usar aqui.

A Zero Trust Exchange opera em 150 data centers ao redor do mundo

Metodologia

A ATOMIK Research entrevistou 1.908 tomadores de decisões sênior (CIOs / CISOs / CDOs / Diretores de Arquitetura de Rede) na EMEA (Reino Unido, Alemanha, França, Países Baixos, Suécia, Itália, Espanha), Américas (EUA, México, Brasil) e APAC (Japão, Índia, Austrália, Singapura). A pesquisa foi conduzida entre 31 de maio e 28 de junho de 2022. A amostra compreendeu 43% de empresas com até 4.999 funcionários, 32% entre 5.000 e 9.999 funcionários e 25% com 10.000 funcionários ou mais.