



The bridge to possible



Relatório de tendências globais de rede de 2022

Edição especial: O status da SASE e a ascensão da rede como serviço (NaaS)



Edição especial:
O status da SASE



Conteúdo

Introdução à SASE	04
O desafio de TI.....	05
A relação entre SD-WAN e SASE.....	07
Recursos desejados da SASE	09
A importância da integração.....	12
Tendências de adoção da SASE.....	15
Modelos de consumo de SASE.....	17
Conclusão sobre a SASE.....	18

Adotando uma estratégia de borda de serviço de acesso seguro (SASE)

O trabalho híbrido demanda uma estratégia de SASE coesa para oferecer uma experiência de usuário confiável e excepcional em qualquer lugar.

Para abordar o crescente interesse e dirimir a confusão no mercado em torno da borda de serviço de acesso seguro (SASE), criamos este adendo especial ao [Relatório de tendências globais de rede de 2022: A ascensão da rede como serviço \(NaaS\)](#).

Impulsionado pelo aumento acentuado do trabalho remoto e da adoção da nuvem híbrida, a SASE (pronuncia-se “sassi”) fornece conectividade segura e contínua para qualquer aplicação, em qualquer rede, de qualquer local ou dispositivo.

A SASE integra funções de rede e segurança em uma solução ou um serviço unificado e nativo de nuvem.

Ao contrário das soluções de segurança tradicionais, ela traz as políticas e a segurança para perto dos usuários finais e das aplicações, que se tornaram cada vez mais distribuídas. Ela expande o Zero Trust e elimina a necessidade de fazer backhaul de dados constantemente para um data center, reduzindo efetivamente as cargas e os gargalos de rede e proporcionando uma experiência de usuário superior.



Como alternativa a uma pilha de segurança tradicional, ela oferece acesso seguro de ponta a ponta, incluindo data center, escritórios remotos, usuários em roaming e outros.

Este adendo destaca as últimas tendências e insights em torno da SASE, com dados de várias pesquisas de mercado e perspectivas obtidas de proeminentes analistas e especialistas do setor. Esperamos que essas informações ajudem você a entender melhor os benefícios e as implicações da SASE ao formular suas estratégias de rede, segurança e nuvem.

– Omri Guelfand, VP de Serviços de Rede da Cisco



“Ainda há muita confusão no mercado sobre o que constitui a SASE. No entanto, o consenso está se alinhando cada vez mais à nossa visão de que a SASE não é uma tecnologia completamente nova, mas sim uma integração das redes atuais, como a WAN definida por software (SD-WAN), a tecnologias de segurança, como gateways de Web seguros (SWG), em uma solução de conectividade segura na nuvem”.

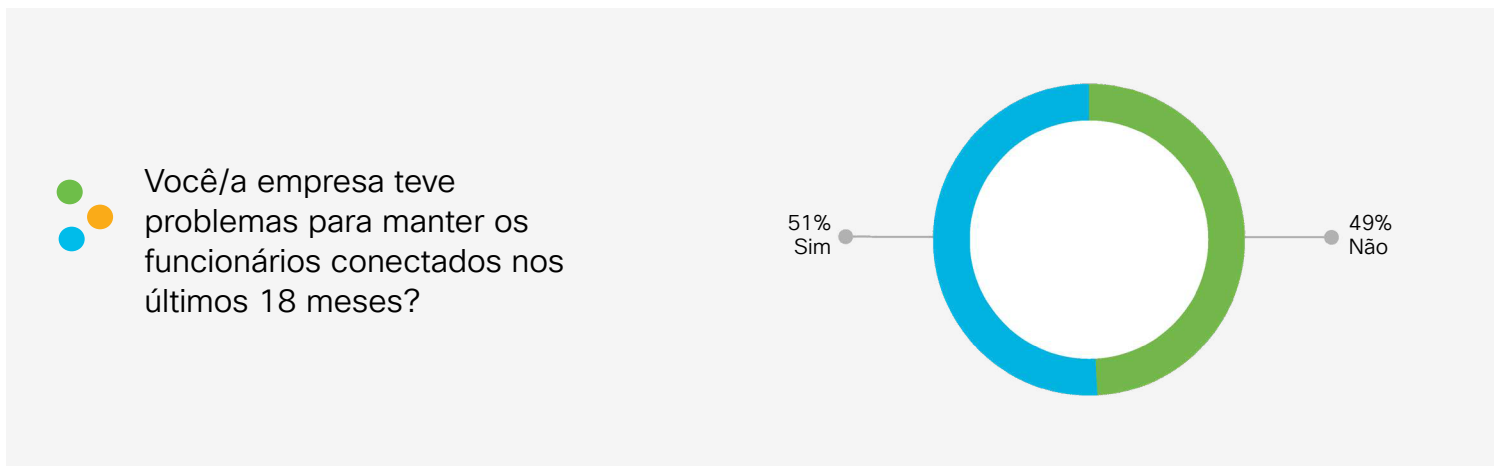
– Dell’Oro Group¹

O desafio da TI: oferecer uma experiência de trabalho híbrido seguro na nuvem (cloud-first)

As duas maiores tendências com as quais as equipes de TI estão lidando hoje são, inegavelmente, a transição contínua para uma estratégia de aplicações multicloud e a adoção de modelos de trabalho híbridos. Com os usuários e as aplicações mais distribuídos do que nunca, a complexidade para conectá-los e protegê-los aumentou significativamente.

A distribuição das aplicações em várias nuvens privadas e públicas agora está amplificada pela imensa distribuição dos trabalhadores e dos espaços de trabalho como consequência do modelo híbrido. Com essa hiperdistribuição, o desafio de tentar manter uma experiência de usuário inclusiva e de alta qualidade contrasta fortemente com o ambiente corporativo que tínhamos antes, que era altamente controlável.

Em pesquisas recentes, 76% das equipes de TI afirmaram que é mais difícil proteger os trabalhadores remotos² e 51% das empresas disseram que tiveram problemas para conectar os trabalhadores aos recursos da empresa nos últimos 18 meses³.



A transição contínua de um modelo de aplicação centrado em data center para um modelo centrado em nuvem e habilitado pela Internet forçou as equipes de TI a repensar totalmente a estratégia de rede. Da mesma forma, as equipes de segurança têm dificuldade para oferecer uma experiência de usuário segura e perfeita quando usuários e aplicações estão fora do local, onde ficam mais suscetíveis à exposição acidental ou a ataques intencionais.

Isso ajuda a explicar o alto nível de interesse em um modelo SASE oferecido na nuvem, que reúne soluções de rede, como SD-WAN e soluções de segurança na nuvem, como borda de serviço de segurança (SSE) e acesso à rede Zero Trust (ZTNA).

A SASE se destina a conectar e proteger usuários e aplicações onde quer que estejam localizados ou hospedados, proporcionando uma experiência de usuário melhor, mais confiável e mais segura. Ela também promete reduzir o custo e a complexidade de TI, melhorar a flexibilidade e o desempenho da rede e, por fim, a experiência de aplicação.



“Em seu ápice de 2020, a pandemia gerou um aumento de 450% no número de funcionários dos EUA trabalhando remotamente em período integral ou em turnos, em comparação com os parâmetros de pré-pandemia. Embora esse número tenha começado a cair, prevemos que as taxas de trabalho remoto de longo prazo se estabeleçam em 200% acima dos parâmetros de pré-pandemia”

– Dell’Oro Group⁴



Resultado:

Uma força de trabalho cada vez mais distribuída e diversificada, que veio para ficar. Implementada corretamente, a SASE conecta e protege usuários e aplicações distribuídas, alinha políticas de rede e segurança e reduz a carga e o risco do gerenciamento de rede e segurança.

A relação entre SD-WAN e SASE

A confusão do mercado em torno da SASE gerou uma série de perguntas sobre as soluções de SD-WAN atuais. A SASE substitui a SD-WAN? Elas se complementam? Ou são soluções totalmente distintas para necessidades diferentes?

A resposta é simples: a SD-WAN é fundamental para a SASE.

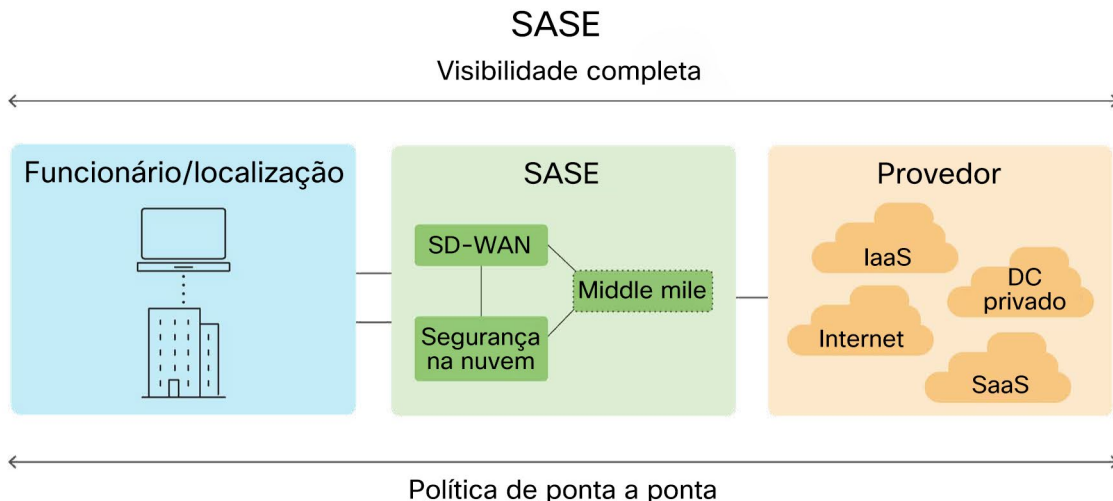
A SASE combina os recursos de segurança nativos da SD-WAN com a segurança centrada na nuvem para conectar e proteger usuários e aplicações, não importa onde estejam localizados ou hospedados. Como uma arquitetura de sobreposição, a SASE não pode oferecer segurança onipresente sem as proteções fornecidas pela SD-WAN, inclusive:

- Viabilizar Network Address Translation (NAT)
- Segmentar a rede em várias sub-redes
- Monitorar e bloquear malware e tráfego mal-intencionado
- Restringir usuários não autorizados
- Evitar conteúdo ou aplicações indesejadas
- Aplicar firewall no tráfego de entrada e no tráfego de VLAN para VLAN indesejado
- Proteger a VPN site a site/em túnel
- Fazer geofencing para controle de acesso baseado em localização

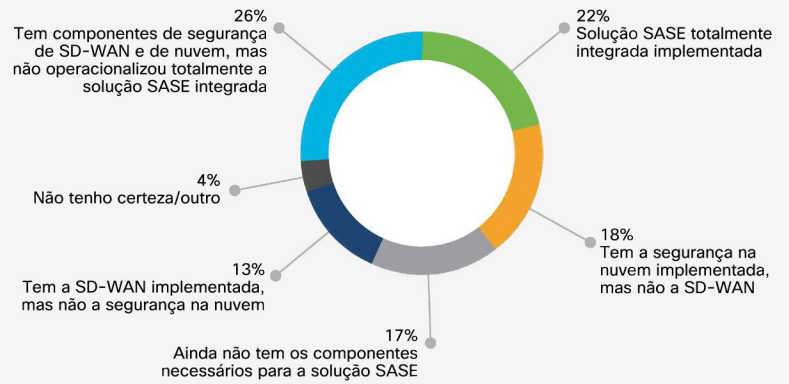


“A SASE não torna a SD-WAN obsoleta. Em vez disso, a SD-WAN é um componente fundamental da SASE. As ofertas da SASE convergem vários recursos de rede e segurança como serviço, como SD-WAN, gateway de Web seguro (SWG), agente de segurança de acesso à nuvem (CASB), firewall de próxima geração (NGFW) e acesso à rede Zero Trust (ZTN)”.

– 2021 Gartner®, Resposta rápida: A SASE substitui a SD-WAN?⁵



Em qual fase você está na sua jornada de adoção da SASE?



Cisco, 2021 Future of Technology Survey; N29,506

As empresas de TI devem começar com a SD-WAN ou com segurança na nuvem? Muitas estão adotando uma abordagem em fases para a implementação da SASE. A maioria está no meio de sua jornada de SASE, com uma combinação de SD-WAN e componentes de segurança na nuvem que ainda precisam ser totalmente integrados ou operacionalizados.

18% das empresas têm segurança na nuvem, mas sem SD-WAN, e 13% têm SD-WAN, mas sem segurança na nuvem.⁶

Resultado:

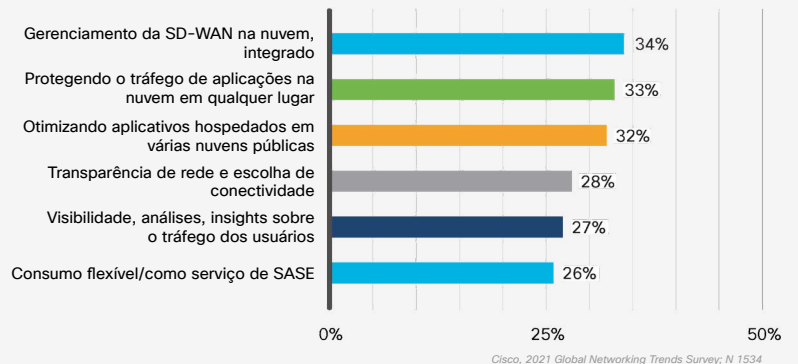
A SD-WAN é um elemento fundamental da SASE que trabalha lado a lado com soluções ou serviços de segurança centrados na nuvem para proteger usuários e dados em domínios locais, de borda e na nuvem.

Recursos desejados da SASE

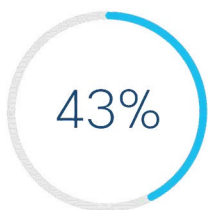
Com a SASE representando a integração de recursos de rede e segurança, 34% das empresas estão priorizando soluções e serviços que oferecem gerenciamento de SD-WAN integrado e na nuvem. Proteger o tráfego de aplicações na nuvem (33%), otimizar aplicações hospedados em várias nuvens públicas (32%) e melhorar a transparência e a flexibilidade da rede (28%) também foram citados como principais prioridades.



Em sua opinião, quais recursos da SASE seriam prioritários para sua empresa?



Para conectar trabalhadores remotos:



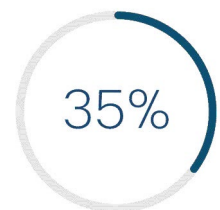
43% das empresas planejam usar a VPN como serviço.



36% estão procurando adotar acesso à rede Zero Trust e recursos de autenticação multifator.



35% estão interessados em clientes unificados baseados em host.



35% desejam estender a SD-WAN a usuários móveis e domésticos.

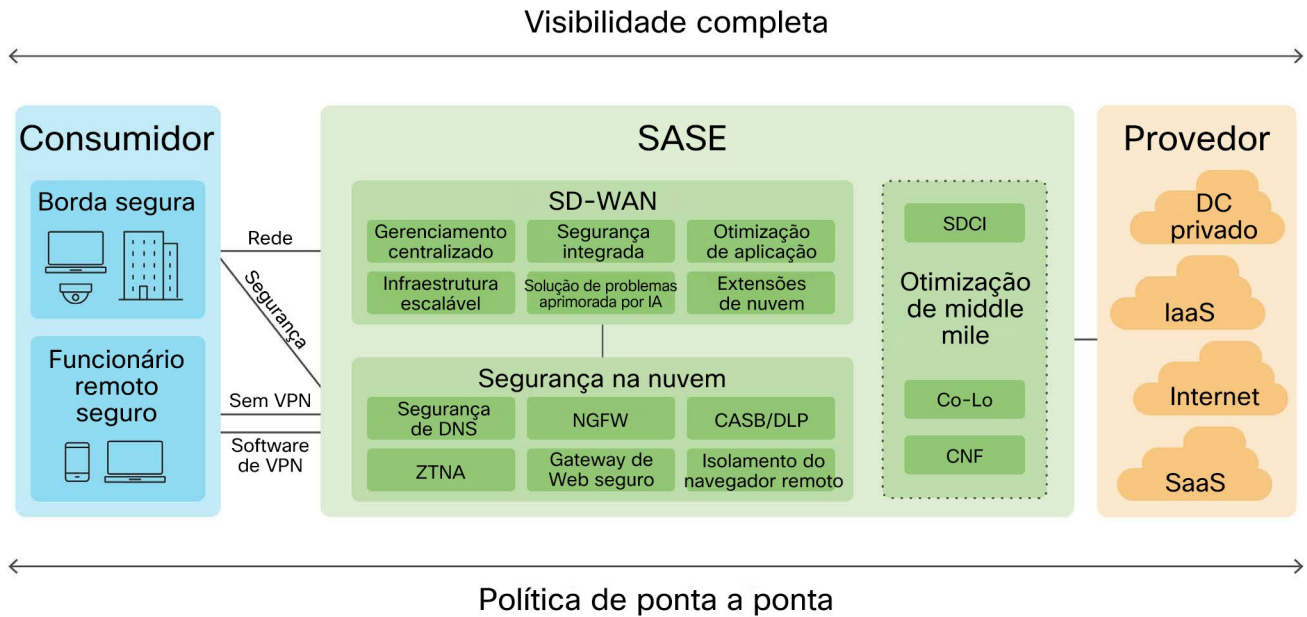
Embora as arquiteturas, as soluções e os serviços de SASE continuem evoluindo, eles são fundamentalmente projetados para reunir alguns ou todos os principais recursos fornecidos pela SD-WAN e pela segurança de nuvem:

SD-WAN	Segurança na nuvem
<p>Gerenciamento centralizado</p> <p>Um painel centralizado e altamente visual que facilita a configuração de dispositivos, gerenciamento de rede, monitoramento e automação. Inclui provisionamento automático (zero-touch) da rede de borda.</p>	<p>Acesso à rede Zero Trust (ZTNA)</p> <p>Uma estrutura de segurança que mitiga o acesso não autorizado, contém violações e reduz o movimento lateral dos invasores na rede. O ZTNA deve ser combinado a um gerenciamento de acesso e uma identidade forte para verificar os usuários e determinar a confiabilidade do dispositivo antes de conceder acesso a aplicações autorizadas.</p>
<p>Extensão de rede de nuvem e otimização de middle mile</p> <p>Extensas integrações on-ramp na nuvem para permitir conectividade contínua e automatizada em qualquer configuração de site para nuvem e de site para site. Inclui conectividade otimizada de middle mile por meio da interconexão de nuvem definida por software (SDCI) e integrações de co-localização.</p>	<p>Gateway de web seguro (SWG)</p> <p>Um gateway que registra e inspeciona o tráfego da Web para fornecer visibilidade total, filtragem de URL, controle de aplicações e proteção contra malware.</p>
<p>Experiência de aplicações</p> <p>A capacidade de monitorar e validar a usabilidade e o desempenho de aplicações da Web. As métricas e cascatas detalhadas mostram a busca e o carregamento sequenciais de componentes da Web para identificar erros e gargalos e entender o impacto no desempenho da aplicação.</p>	<p>Firewall na nuvem com IPS (Sistema de prevenção de violações)</p> <p>Serviços baseados em software e implantados na nuvem que ajudam a gerenciar e inspecionar o tráfego de rede.</p>
<p>Infraestrutura flexível e escalável</p> <p>Uma ampla variedade de plataformas físicas e virtuais que oferecem alta disponibilidade e taxa de transferência, opções de porta multigigabit, links de celular 5G e recursos avançados de criptografia. Otimiza o tráfego de WAN selecionando dinamicamente os links de WAN mais eficientes que atendem aos requisitos de nível de serviço.</p>	<p>Agente de segurança de acesso à nuvem (CASB)</p> <p>Software que detecta e informa sobre aplicações de nuvem em uso na rede, expondo shadow IT e permitindo que aplicações SaaS arriscadas e ações específicas, como postagens e uploads, sejam bloqueadas.</p>
<p>Solução de problemas aprimorada por IA</p> <p>IA/ML robusto para otimizar o desempenho da rede, automatizar tarefas manuais de rotina e acelerar a solução de problemas. Fornece alertas inteligentes, autocorreção e recursos de redirecionamento preditivo da Internet.</p>	<p>Prevenção de perda de dados (DLP)</p> <p>Software que analisa dados em linha para fornecer visibilidade e controle sobre dados confidenciais que estão sendo enviados para fora da rede da empresa ou da nuvem.</p>
<p>Segurança integrada</p> <p>Recursos de segurança robustos que trabalham lado a lado com a segurança na nuvem para proteger filiais, usuários domésticos e aplicações na nuvem contra infiltrações.</p>	<p>Isolamento do navegador remoto (RBI)</p> <p>Software que isola o tráfego da Web dos dispositivos do usuário para mitigar o risco de ameaças enviadas pelo navegador.</p>
<p>Gerenciamento de política baseado em identidade</p> <p>Gerenciamento de microssegmentação e política baseado em identidade em vários locais e domínios.</p>	<p>Segurança na camada de DNS</p> <p>Software que atua como a primeira linha de defesa contra ameaças na Internet, bloqueando solicitações de DNS mal-intencionadas antes mesmo que uma conexão com um endereço IP seja estabelecida. A segurança robusta do DNS pode reduzir bastante o número de ameaças das quais a equipe de segurança precisa fazer a triagem diariamente.</p>
<p>Insights avançados</p> <p>Visibilidade aprimorada no ambiente de aplicações, na Internet, na nuvem e no SaaS com análise abrangente, hop-by-hop. Permite o isolamento de domínios de falha e fornece insights acionáveis para acelerar a solução de problemas e minimizar ou eliminar o impacto para os usuários.</p>	<p>Inteligência de ameaças</p> <p>Pesquisadores de ameaças, engenheiros e cientistas de dados que usam telemetria e sistemas sofisticados para criar uma inteligência de ameaças precisa, rápida e acionável para identificar ameaças emergentes, descobrir novas vulnerabilidades e interditar ameaças circulantes antes que elas se espalhem, com conjuntos de regras que aceitam as ferramentas na pilha de segurança.</p>

Além de integrar a SD-WAN e os recursos de segurança na nuvem, os modelos SASE podem ajudar a quebrar silos operacionais e promover maior alinhamento entre as equipes de rede e segurança. Com políticas padronizadas, telemetria compartilhada e alertas coordenados em todos os componentes de segurança e rede, a SASE permite que as equipes de NetOps e SecOps melhorem a eficiência, a visibilidade e a proteção da TI.

Com isso em mente, é importante que as empresas tenham uma estratégia de SASE abrangente que acomode as metas de NetOps e SecOps, aumente o alinhamento operacional e seja capaz de atender às necessidades da empresa no futuro próximo.

SASE: detalhe



“Até 2024, 30% das empresas vão adotar recursos de gateway da Web seguro (SWG) na nuvem, agente de segurança de acesso à nuvem (CASB), acesso à rede Zero Trust (ZTNA) e firewall de filial como serviço (FWaaS) do mesmo fornecedor, um número bem maior que os menos de 5% em 2020”.

– Gartner⁷



Resultado:

À medida que avaliam as estratégias e ofertas de SASE, as empresas buscam soluções e serviços que forneçam os recursos fundamentais de SD-WAN e segurança na nuvem para atender às necessidades atuais e em evolução.



A importância da integração

As empresas modernas contam com vários ambientes de rede (redes de data center, redes locais, redes de longa distância) e soluções de segurança (firewalls, gateways e controle de acesso para sistemas locais e na nuvem). Por meio de integrações de tecnologia e serviços, a SASE pode fornecer visibilidade, orquestração de políticas e proteção em todos eles.

Com o objetivo final de conectar usuários e aplicações com segurança onde quer que estejam localizados ou hospedados, essas integrações também ajudam a:

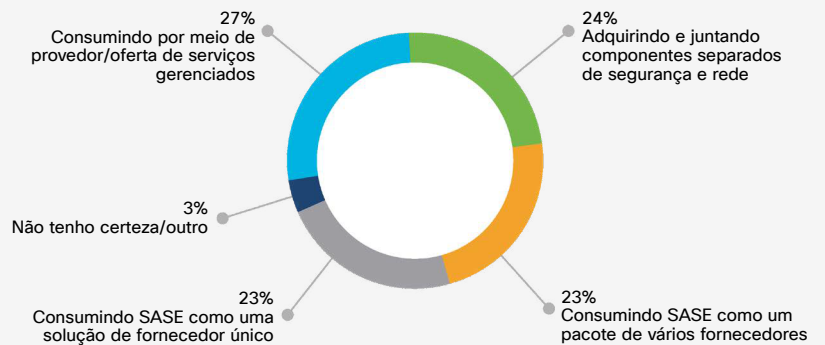
- Reduzir o volume de incidentes de segurança.
- Melhorar a padronização e a aplicação de políticas.
- Acelerar a identificação e a resolução de problemas.
- Apoiar a conformidade regional e os requisitos de dados.
- Simplificar o monitoramento e o gerenciamento de sistemas.
- Reduzir os custos de capital e operacionais.

“Existem dois principais tipos de implementação de SASE no mercado, a unificada e a desagregada. A implementação unificada consiste em plataformas SASE de fornecedor único e são fortemente integradas. A implementação desagregada é uma implementação de vários fornecedores ou vários produtos com menos integração em comparação com a variante unificada”.

– Dell’Oro Group⁹



Como você vai implantar e operacionalizar sua solução SASE?



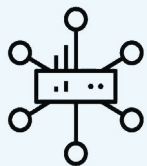
Cisco, 2021 Future of Technology Survey; N 29,506

Com o surgimento de soluções e serviços de um único fornecedor e de vários fornecedores, bem como a possibilidade de ter arquiteturas personalizadas que unem várias soluções pontuais, as empresas contam com várias opções de como implantar e operacionalizar a SASE.

Como a criação e a integração de uma solução personalizada ou a operacionalização de um pacote SASE de vários fornecedores pode apresentar complexidades indesejadas, desafios operacionais e vulnerabilidades de segurança, muitos (50%) estão buscando uma solução unificada e/ou gerenciada de um único fornecedor.

- 70% concordam ou concordam fortemente que se tornou cada vez mais complexo gerenciar uma rede de vários fornecedores e uma pilha de segurança com eficiência.
- 26% têm recursos de segurança na nuvem e SD-WAN, mas não os operacionalizaram totalmente e os integraram em um modelo SASE completo.¹⁰

Seja uma arquitetura personalizada, um pacote de vários fornecedores, um serviço totalmente gerenciado de um único fornecedor ou uma variação dele, toda solução SASE deve fornecer melhor alinhamento e integração entre:



SD-WAN e segurança de nuvem

- Automatize o roteamento de tráfego entre o dispositivo SD-WAN e os pontos de presença (PoPs) de segurança na nuvem.
- Redirecione automaticamente o tráfego para um PoP alternativo para ter resiliência quando houver um problema de desempenho.
- Use análises preditivas viabilizadas por IA para redirecionar automaticamente o tráfego para PoPs alternativos, antes que a experiência do usuário seja afetada.



Equipes de NetOps e SecOps

- Compartilhe continuamente políticas de segurança (como autorizações de acesso e segmentação) entre as implementações de SD-WAN e de segurança na nuvem.
- Permita a troca de dados entre SD-WAN e plataformas de gerenciamento de segurança de nuvem para oferecer visibilidade constante de políticas e eventos.
- Estenda e propague blocos de rede corporativa (como VPNs e marcas de grupo de segurança) e políticas em plataformas de segurança na nuvem.
- Use a autenticação administrativa de logon único (SSO) nas plataformas de SD-WAN e gerenciamento de segurança na nuvem.



Usuários finais e aplicações

- Habilite a conectividade direta entre serviços de SD-WAN, middle mile (como SDCI), multicloud e SaaS.
- Monitore e otimize a experiência do usuário com total visibilidade e análise na SD-WAN, nos PoPs de segurança na nuvem e nas conexões IaaS/SaaS.

“É impossível criar uma rede boa sem integrar a segurança. É preciso olhar para a segurança de forma holística, desde o endpoint até a rede e a aplicação. Com a rede como serviço, preciso que o provedor assuma a responsabilidade pela rede e pela segurança. Se eles assumem apenas a responsabilidade pela rede, preciso da visibilidade e do controle necessários para garantir proteção total e rápida mitigação de ameaças. No mundo ideal, o provedor faria ambos a comunicação em rede e segurança muito bem”

– Diretor de infraestrutura de TI, empresa global de produtos de consumo

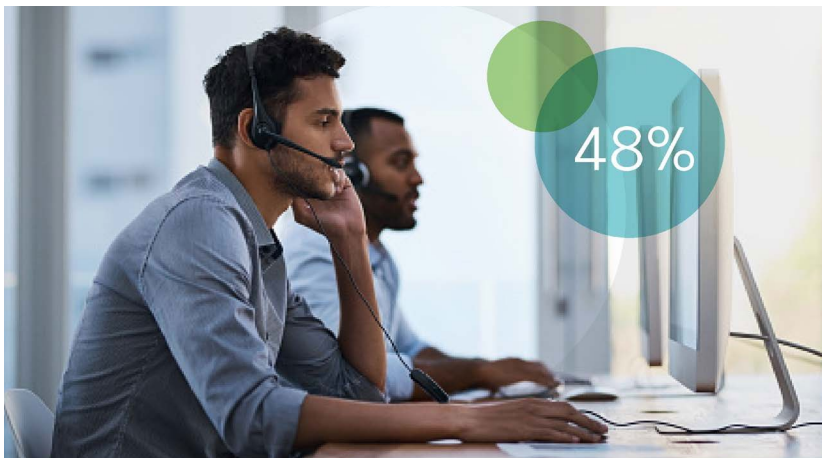
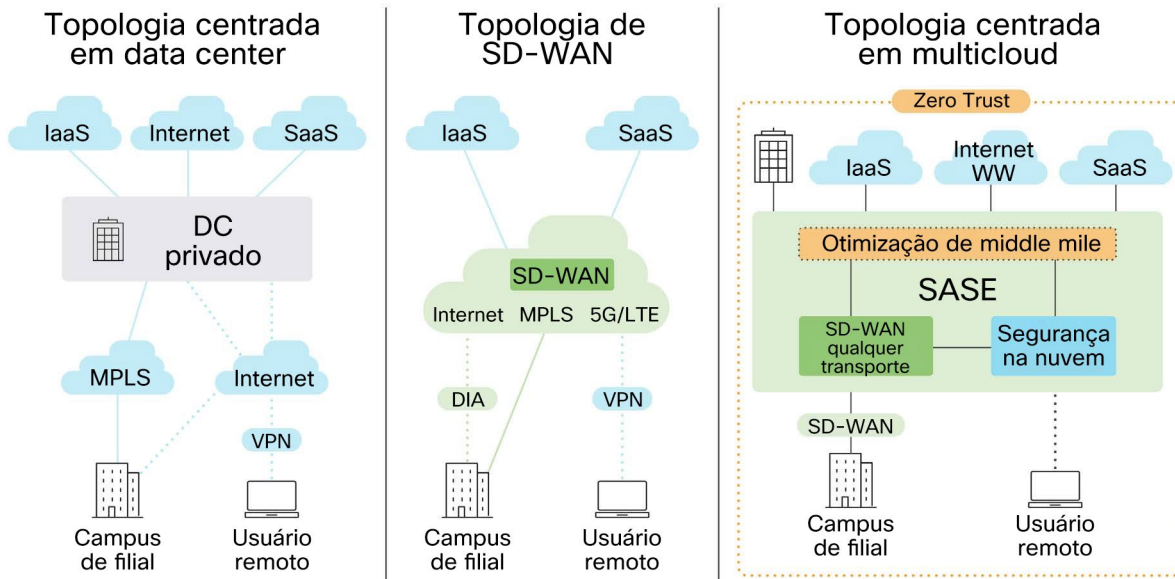
- **Resultado:**
- Sejam personalizados ou disponibilizados por um ou mais fornecedores, as soluções e serviços SASE precisam fornecer integração total entre a SD-WAN e os sistemas de segurança de nuvem, para proporcionar uma experiência de usuário segura e agilizar a colaboração entre NetOps e SecOps.

Tendências de adoção da SASE

Como acontece com qualquer decisão de tecnologia, o modelo de SASE correto e a melhor abordagem de implantação serão exclusivos para cada empresa. As soluções de rede e segurança já implementadas, bem como as estratégias operacionais abrangentes e as prioridades de negócios, devem ser fatores determinantes em qualquer decisão sobre SASE. Iniciativas importantes, demandas regulatórias, fusões e aquisições, operações da cadeia de suprimentos e requisitos de resiliência de negócios também devem ser considerados.

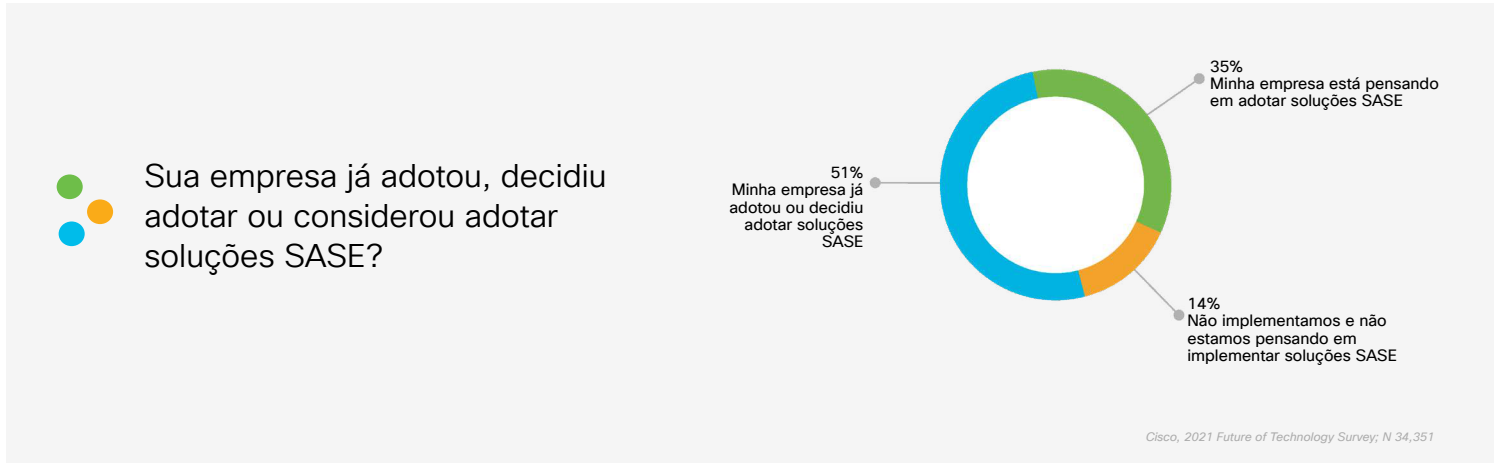
As empresas que migram de um modelo de aplicação centrado em data center para um modelo centrado na nuvem ou multicloud podem iniciar a jornada SASE com a SD-WAN, por exemplo, seguida de otimização de middle mile e integração de segurança na nuvem.

De topologia centrada em DC para centrada em multicloud



48% das empresas interessadas em SASE vão começar com segurança, 31% vão começar com a rede e 21% planejam abordar segurança e rede simultaneamente.⁸

Independentemente do modelo específico ou da abordagem de implantação, muitas empresas afirmam que já estão dando andamento à adoção da SASE: 86% das empresas consideram adotar ou já adotaram a SASE.¹¹



“Até 2025, pelo menos 60% das empresas terão estratégias e cronogramas explícitos para adoção da SASE, abrangendo acesso de usuário, filial e borda, acima dos 10% em 2020”
– Gartner¹²

Resultado:
As abordagens de implantação da SASE são influenciadas pelos atuais ciclos de vida de infraestrutura e pelas prioridades operacionais e iniciativas de negócios. As equipes de TI precisam adotar uma abordagem de planejamento estratégico destinada a construir incrementalmente uma arquitetura SASE completa.

Modelos de consumo da SASE

Existem três principais modelos de consumo de soluções e serviços de SASE. Embora esses modelos de consumo tenham impactos variados nas equipes e operações internas, todos eles quebram os silos tradicionais de rede e segurança. Como resultado, a SASE pode ser um recurso que força a melhoria do alinhamento e a eficiência operacional.



Como um serviço

Para aqueles que desejam uma implantação rápida, impacto mínimo nas operações e na equipe e o risco reduzido que acompanha os SLAs, a SASE como serviço oferece uma série de recursos totalmente integrados e entregues na nuvem com um único painel e suporte completo ao ciclo de vida. 26% das empresas citam a SASE como um serviço como o modelo de consumo preferido.



Híbrida ou cogerenciada

As empresas que ainda não estão prontas para um modelo completo como serviço ou que desejam mais personalização do que esses serviços oferecem podem adotar uma abordagem híbrida. Isso envolve a integração de recursos de segurança na nuvem com uma solução de SD-WAN atual e/ou o compartilhamento de rede e responsabilidades de segurança com um provedor de serviços gerenciados. Essas abordagens híbridas fornecem segurança e suporte adicionais e permitem que as equipes de TI mantenham uma medida de visibilidade e controle, enquanto reduzem as demandas gerais de gerenciamento do ciclo de vida.



Altamente personalizada ou DIY

As empresas que desejam total personalização e controle da rede e da área de cobertura de segurança podem criar, integrar e gerenciar recursos SASE por conta própria. Esse nível de personalização e controle normalmente vem à custa da velocidade e agilidade; requer gerenciamento adicional do ciclo de vida do hardware, do software e das licenças e demanda especialistas extras em segurança e conformidade. Esta é uma boa opção para empresas com demandas muito específicas e uma rede e equipe atuais que podem atender aos requisitos de arquitetura e operacionais da SASE.

Leia sobre as lições aprendidas no [Caso de uso de implantação da borda de serviço de acesso seguro \(SASE\) da Cisco](#).



Resultado:

Há vários modelos de consumo de SASE com impactos operacionais variados. O modelo certo para cada empresa depende de vários fatores, incluindo o tamanho, o conjunto de habilidades e a largura de banda da equipe interna de TI e a priorização de necessidades específicas, velocidade, agilidade, visibilidade e controle.



Conclusão sobre a SASE

As arquiteturas, as soluções e os serviços de SASE oferecem conectividade segura entre qualquer usuário e aplicação, não importa onde estejam localizados ou hospedados. Mas a jornada para a SASE será única em cada empresa. O modelo e a abordagem corretos vão depender dos atuais investimentos em tecnologia, bem como das prioridades de TI e de negócios.

A Cisco e seu ecossistema de parceiros podem ajudar a atender às suas necessidades exclusivas de rede e segurança com a solução de SASE mais completa, flexível e resiliente do mercado.

Você pode escolher no nosso amplo portfólio de SASE, que combina a melhor rede da categoria, conectividade de cliente e segurança e recursos exclusivos de observabilidade da Internet para oferecer os resultados de que você precisa. Você também pode escolher entre uma variedade de modelos de implantação e consumo de SASE simples e flexíveis, que atendem a uma variedade de situações e requisitos.

Nossa infraestrutura de segurança em nuvem global altamente disponível fornece acesso seguro onde quer que os usuários e as aplicações residam. E nossas soluções de SD-WAN líderes de mercado fornecem a agilidade e os recursos necessários para proporcionar experiências de alta qualidade para seus usuários, constantemente. Juntas, nossas soluções de segurança na nuvem e SD-WAN oferecem os recursos de SASE mais completos, integrados e exclusivos do setor.

No futuro, a Cisco vai inovar a SASE em ritmo acelerado por meio de integrações e aprimoramentos contínuos dos recursos. Estamos desenvolvendo nossas ofertas para fornecer os serviços de SASE mais flexíveis e de mais fácil consumo para você.

Para saber mais, acesse o [Centro de recursos de SASE da Cisco](#).

A Cisco foi reconhecida como líder no Quadrante Mágico do Gartner™ em Infraestrutura de WAN Edge, pela capacidade de execução e abrangência de visão.¹³



Recursos adicionais e assistência

[Link para o roadmap da SASE >](#)

[Encontre um parceiro da Cisco >](#)

[Fale com a equipe de vendas da Cisco >](#)

A Gartner não endossa nenhum fornecedor, produto ou serviço descrito em suas publicações de pesquisa, e não aconselha usuários de tecnologia a selecionarem apenas os fornecedores com as classificações mais elevadas ou outra designação. As publicações de pesquisa da Gartner consistem em opiniões da empresa de pesquisa da Gartner's Research & Advisory e não devem ser interpretadas como declarações de fatos. A Gartner não oferece nenhuma garantia, expressa ou implícita, com respeito a essa pesquisa, incluindo garantias de comerciabilidade ou adequação a uma finalidade específica. GARTNER e MAGIC QUADRANT são marcas comerciais e marcas de serviço da Gartner, Inc. e/ou suas afiliadas e são usadas aqui com permissão. Todos os direitos reservados.

Fontes sobre SASE

1. Advanced Research Report: SASE Market Forecast, Vol. 2, No. 1, Dell'Oro Group, setembro de 2021.
2. The State of Security 2021, Splunk, fevereiro de 2021.
3. Future of Technology, Cisco, novembro de 2021.
4. Advanced Research Report: SASE Market Forecast, Vol. 2, No. 1, Dell'Oro Group, setembro de 2021.
5. Gartner Quick Answer: Does SASE Replace SD-WAN?, Andrew Lerner, Neil MacDonald, dezembro de 2021.
6. Relatório de tendências globais de rede da Cisco para 2022: a ascensão da rede como serviço, Cisco, outubro de 2021.
7. Gartner 2021 Strategic Roadmap for SASE Convergence, março de 2021.
8. SASE Trends: Plans Coalesce but Convergence Will Be Phased, ESG Research Report, dezembro de 2021.
9. Advanced Research Report: SASE Market Forecast, Vol. 2, No. 1, Dell'Oro Group, setembro de 2021.
10. Relatório da Cisco de tendências globais de rede de 2022: a ascensão da rede como serviço, Cisco, outubro de 2021.
11. Future of Technology, Cisco, novembro de 2021.
12. 2021 Strategic Roadmap for SASE Convergence, Gartner, março de 2021.
13. Quadrante Mágico do Gartner de WAN Edge Infrastructure, setembro de 2021.



A ascensão da rede como serviço (NaaS) como





Conteúdo

Dar as boas-vindas	22
Principais descobertas	23
Um modelo de rede diferente	25
Como resolver desafios, como oferecer vantagens	27
Como a NaaS muda as operações de rede	29
Funções, responsabilidades e conjuntos de habilidades	31
Preocupações e hesitações	33
Tendências de adesão	35
Como escolher um provedor de NaaS	36
SASE e as diferentes nuances da NaaS	38
Conclusão	40
Recursos adicionais e assistência	40
Sobre este relatório	41
Permissões para usar este relatório	42



Dar as boas-vindas

Bem-vindo ao relatório de tendências globais de rede para 2022: a ascensão da rede como serviço (NaaS).

Que momento extraordinário estamos vivenciando, tanto como humanos quanto como profissionais de rede. No ano passado, líderes de TI e profissionais de rede foram encarregados de viabilizar o trabalho remoto, proteger os dados em um cenário de computação mais distribuído e fornecer novos serviços para usuários, clientes e parceiros. Muitas empresas intensificaram seus esforços de transformação digital para atender a esses novos requisitos, aproveitando a nuvem e o software como serviço (SaaS) para obter maior flexibilidade, agilidade e velocidade.

Em nosso [relatório de tendências globais de rede para 2021](#), destacamos as maneiras como as tecnologias de rede estão sendo usadas para melhorar a resiliência de negócios – independentemente das circunstâncias.

No relatório deste ano, nós nos concentramos em uma nova tendência que tem grandes implicações para o futuro: a rede como serviço.

Seguindo os modelos como serviço (aaS) cada vez mais populares, como SaaS e infraestrutura como serviço (IaaS), a NaaS mudará constantemente a maneira como muitas empresas adquirem, fornecem e gerenciam os recursos de rede. Para saber mais, falamos com 20 líderes de TI e entrevistamos 1.534 profissionais de TI em 13 países sobre como eles consideram a NaaS, seus pontos fortes e suas limitações, e se planejam aderir ao novo modelo de consumo de rede.

Esperamos que os dados, as perspectivas e as diretrizes deste relatório ajudem você a entender melhor as vantagens e implicações da NaaS, à medida que você desenvolve suas estratégias de rede.

– James Mobley, serviços de rede SVP, Cisco



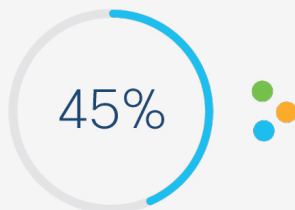


Principais descobertas

É uma proposta extraordinária transformar completamente a sua maneira de consumir e operar a rede. Você precisa de bons motivos comerciais e tecnológicos para fazer essa transição para um modelo como serviço. E você também precisa de parceiros confiáveis com quem possa contar para manter a sua empresa funcionando. Ainda assim, muitas empresas estão altamente motivadas para fazer a mudança. Estas são algumas descobertas importantes de nossa pesquisa sobre NaaS para 2022:

Primeira principal descoberta: desafios

Se resiliência e agilidade são um problema, para muitos, a NaaS é a resposta.



- A resposta a interrupções (45%) e a adaptação a novas necessidades comerciais (40%) são citadas como os principais desafios de rede para 2021.
- Ao mesmo tempo, as equipes de TI reconhecem as principais vantagens da NaaS, como liberá-las para oferecer inovação e valor comercial (46%). Outros 40% reconhecem que a NaaS melhora a resposta a interrupções e 34% que melhora a agilidade da rede.

Segunda principal descoberta: vantagens

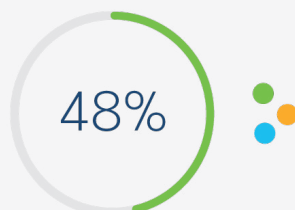
Grandes expectativas: o acesso rápido às tecnologias mais recentes é o grande prêmio.



- A tecnologia continua evoluindo mais rapidamente do que as empresas podem aderi-la. 35% dos entrevistados reconhecem a necessidade de implantar continuamente as tecnologias de rede mais recentes, como Wi-Fi 6, WAN definida por software (SD-WAN), borda de serviço de acesso seguro (SASE), 5G, IA e outras como o principal indicador para NaaS.

Terceira principal descoberta: operações

A NaaS é excelente, mas apenas se ajudar a equipe de rede a cumprir os contratos de nível de serviço (SLAs).

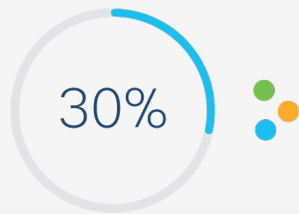


- Os principais serviços exigidos dos provedores de NaaS são gerenciamento do ciclo de vida da rede (48%), resiliência da rede (42%), bem como monitoramento e solução de problemas para cumprir os SLAs (38%).



Quarta principal descoberta: preocupações

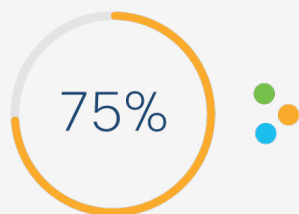
Mas nem tudo são flores. Existem algumas preocupações em abrir mão do controle e dos custos.



- As preocupações variam desde se a NaaS pode atender às novas demandas inéditas (30%) até a perda do controle de segurança (26%).
- O custo e a disrupção da transição também têm uma classificação elevada (28%).

Quinta principal descoberta: funções

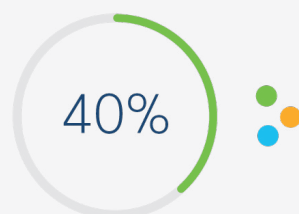
A NaaS abre novos horizontes para os profissionais de TI, mas eles precisam atualizar seus conhecimentos.



- Mais de 75% das empresas concordam ou concordam plenamente que a NaaS dará às equipes de TI oportunidades de aprimorar suas habilidades.
- No entanto, hoje, apenas uma a cada quatro empresas está propensa a confiar em sua própria equipe de TI, em vez de um integrador de sistemas, provedor de serviços gerenciados ou fornecedor de NaaS para converter as necessidades comerciais em políticas técnicas.

Sexta principal descoberta: adesão

Existem várias maneiras de começar a usar a NaaS e uma delas é a SASE.



- A solução SASE é um ponto de entrada provável para a NaaS, pois 40% das empresas mencionam o acesso multicloud, e 34% mencionam a segurança como uma boa opção para a NaaS.
- 49% das empresas planejam começar a usar a NaaS durante um ciclo de reciclagem ou atualização, e 34% afirmaram que começariam com a adaptação de um site atual.



Um modelo de rede diferente

Depois de mais de 18 meses de interrupção e adaptação, o papel desempenhado pelas tecnologias de rede na sobrevivência e no sucesso das empresas nunca foi tão evidente – ou tão fundamental. Já um facilitador fundamental do trabalho remoto, agora as redes estão sendo solicitadas a oferecer suporte a locais de trabalho mais seguros, modelos de trabalho híbridos e operações de

negócios em evolução. Para tanto, elas precisam funcionar perfeitamente em ambientes locais, multicloud e de borda. Elas precisam oferecer uma experiência segura e estável para todos os usuários, independentemente de localização, dispositivo ou método de conectividade. E elas precisam oferecer suporte a aplicações orientadas a microsserviços tradicionais e modernos.

Como os recursos e a largura de banda costumam ser limitados, muitos líderes de TI e de rede estão investigando a NaaS como alternativa para resolver esses desafios. Mas o que isso significa exatamente?

Quando perguntamos aos líderes de TI como eles definem a NaaS, ficou claro rapidamente que ela tem significados diferentes para pessoas diferentes. Na verdade, em nossa pesquisa, surpreendentes 36% dos entrevistados afirmaram já ter a NaaS. Embora essa porcentagem possa parecer alta para uma tecnologia nova, em nossas entrevistas percebemos que muitos consideram ter a NaaS, se alguma parte de sua rede for gerenciada por um provedor de terceiros. Acreditamos que esta definição é muito ampla e precisa ser mais específica.



NaaS é um modelo de consumo baseado no uso e habilitado para a nuvem que permite aos usuários adquirir e orquestrar recursos de rede sem possuir, criar ou manter sua própria infraestrutura.



"As empresas estão tentando determinar a combinação certa de recursos internos e fornecidos por parceiros. Muitas estão optando por investir em funcionários, análise, observabilidade e automação, e estão pensando seriamente em como aproveitar fornecedores estratégicos para transferir o gerenciamento e a manutenção da infraestrutura."

– Mary Turner, vice-presidente de pesquisa, IDC



A NaaS pode fornecer um modelo de consumo alternativo para uma ampla gama de elementos de rede, incluindo LANs com e sem fio, WANs e VPNs, bem como ambientes de filial, data center, borda, multicloud e nuvem híbrida. Pode ser usada para fornecer novos modelos de rede, como SASE. Pode viabilizar mudanças nos modelos organizacionais, como a migração para o trabalho híbrido. E como serviço sob demanda, a NaaS pode permitir que as equipes de TI se adaptem com mais facilidade, implantem novos serviços rapidamente e otimizem o equilíbrio entre CapEx e OpEx.

Para alguns líderes de TI com quem conversamos, a NaaS representa uma forma de rede nova e melhor que é muito necessária.

Eles reconhecem que estão ficando para trás e perdendo a confiança dos usuários. E eles acreditam que a NaaS pode ajudá-los a obter as tecnologias mais recentes, atender a um conjunto crescente de requisitos e acompanhar o ritmo acelerado dos negócios.



"Com o nível de complexidade da rede tão alto, a velocidade com que as empresas precisam responder às mudanças do mercado e o amplo alcance das redes modernas, muitas pessoas estão percebendo: 'não aguentamos mais essa situação e precisamos de ajuda'".

– Mark Leary, diretor de pesquisa, análise de rede, IDC



Resultado:

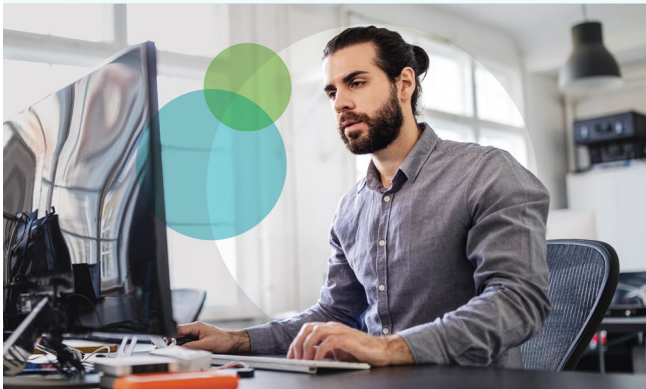
A adesão à NaaS deve aumentar a uma taxa composta de crescimento anual de 40,7% de 2021 a 2027.¹

Como resolver desafios, como oferecer vantagens

Optar por aderir a um modelo de NaaS, em última análise, resume-se aos desafios comerciais e tecnológicos que ele resolve, bem como às vantagens que oferece.

Para as empresas que entrevistamos, a agilidade continua sendo a prioridade. Quando perguntamos sobre os maiores desafios comerciais que a rede deve enfrentar, quase 50% dos profissionais de TI disseram a resposta a interrupções e 40% disseram a adaptação a novos aplicativos corporativos e projetos de negócios. Mais de um terço dos entrevistados identificou a necessidade de agilidade de rede como indicador importante para a NaaS, e metade dos entrevistados disse que espera que a NaaS permita oferecer maior inovação e valor comercial.

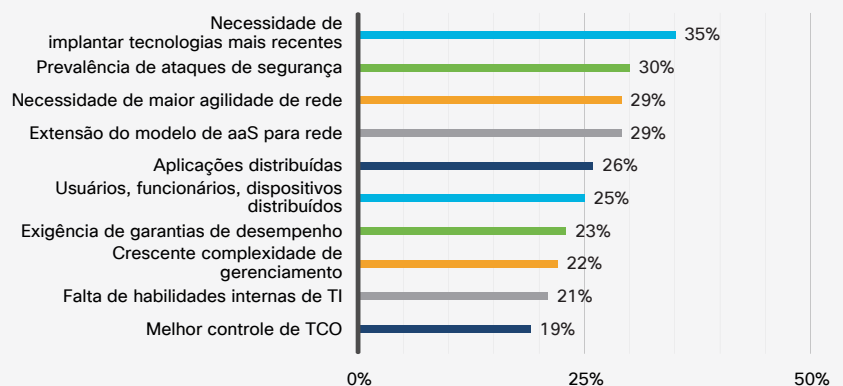
Como parte dos esforços para serem mais ágeis, muitas empresas de TI estão mudando suas aplicações e serviços para a nuvem, o que pode apresentar novos desafios de segurança, administração e conformidade.



De acordo com os profissionais de TI entrevistados, os maiores desafios tecnológicos que eles enfrentam no gerenciamento das redes atualmente incluem conectar-se a várias nuvens (36%); proteger a rede, os usuários e as aplicações (34%); bem como identificar as causas do problema e corrigir os problemas de segurança ou desempenho rapidamente (31%).

Ao mesmo tempo, um terço dos entrevistados identificou a necessidade de implantar continuamente as tecnologias de rede mais recentes (como Wi-Fi 6, SD-WAN, SASE, 5G, IA etc.) como uma motivação-chave para migrar para a NaaS, e um terço mencionou a capacidade de defesa contra ameaças à segurança, que estão se tornando mais frequentes e sofisticadas.

O que provavelmente faria com que sua empresa mudasse para um modelo de NaaS?





"Nossos executivos não veem vantagens em minha equipe configurar dispositivos ou operar a infraestrutura. Eles querem que a TI pense em termos de objetivos de negócios. Usar serviços externos para operações básicas permite que minha equipe se aproxime dos resultados de negócios."

– Diretor de infraestrutura de TI, empresa global de produtos de consumo

Quando perguntamos sobre as principais vantagens que os profissionais de TI esperam da NaaS, os tomadores de decisão primários mencionaram a capacidade de se concentrar no fornecimento de valor comercial, em vez do gerenciamento de infraestrutura cotidiano.

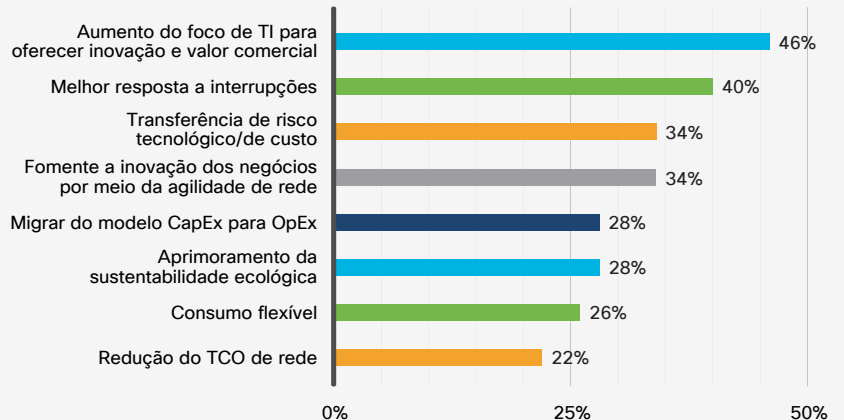
Melhorar a resposta às interrupções de rede e segurança foi outra vantagem com classificação elevada da NaaS, conforme citado por 45% dos profissionais de rede e 40% dos tomadores de decisão primários. Embora já esperássemos a priorização das melhorias de segurança, ficamos interessados em saber que mais de 25% dos profissionais de rede e 33% dos tomadores de decisão primários identificaram a sustentabilidade ecológica aprimorada como uma grande vantagem da NaaS.

Ainda mais surpreendente foi a baixa classificação das vantagens financeiras da NaaS.

Com um modelo de consumo flexível e os preços baseados em assinatura, a NaaS permite que as equipes de TI mudem os gastos de CapEx para OpEx e evitem grandes investimentos recorrentes em infraestrutura de rede. Em vez disso, os gastos se tornam mais estáveis e previsíveis, e as empresas pagam apenas pelos recursos que usam. E, ainda assim, esses benefícios fiscais receberam uma classificação muito menor dos líderes de TI e profissionais de rede, em comparação às vantagens de agilidade, inovação e transferência de gerenciamento da NaaS.



Na sua opinião, quais são as três principais vantagens comerciais que podem ser originadas pelo uso de um modelo de NaaS?



Resultado:

O TCO não está na lista de prioridades quando se trata de NaaS, porque as empresas estão muito mais preocupadas em oferecer valor comercial e responder rapidamente às interrupções. 68% dos líderes de TI concordam ou concordam plenamente que a NaaS livrará as equipes do gerenciamento de rede cotidiano, permitindo mais tempo para se concentrarem em oferecer inovação e valor comercial.



Como a NaaS muda as operações de rede (NetOps)

Uma preocupação comum que ouvimos sobre a NaaS é que ela exige uma transferência completa das operações de rede, atribuindo todas as responsabilidades ao provedor de NaaS e deixando nada para a equipe de NetOps da empresa fazer. Mas a realidade é que a NaaS não é um jogo de tudo ou nada, quando se trata de responsabilidade operacional.

Em um modelo de NaaS, o provedor assume a responsabilidade por todos os aspectos do gerenciamento do ciclo de vida da rede. Isso inclui implantação, integração,

controle, atualização, monitoramento e reparo de todos os elementos da infraestrutura de rede – incluindo qualquer um dos equipamentos locais dos clientes – necessários para entregar os resultados contratuais. Os resultados podem incluir o número de usuários, sites, provedores de nuvem e aplicações conectados, bem como os níveis de serviço combinados, largura de banda, desempenho das aplicações, disposições de segurança, conformidade e outros requisitos.

Então, o que resta para gerenciar? A equipe de NetOps do cliente de NaaS poderá concentrar mais tempo nas atividades principais ou de valor agregado.

Isso pode incluir, por exemplo, definir e monitorar os resultados de rede desejados, como políticas de acesso dos usuários e das aplicações, bem como os níveis de desempenho das aplicações. Ao monitorar o desempenho e os insights da rede, a equipe de NetOps do cliente pode adaptar e otimizar continuamente as políticas e comportamentos de rede em todos os domínios.



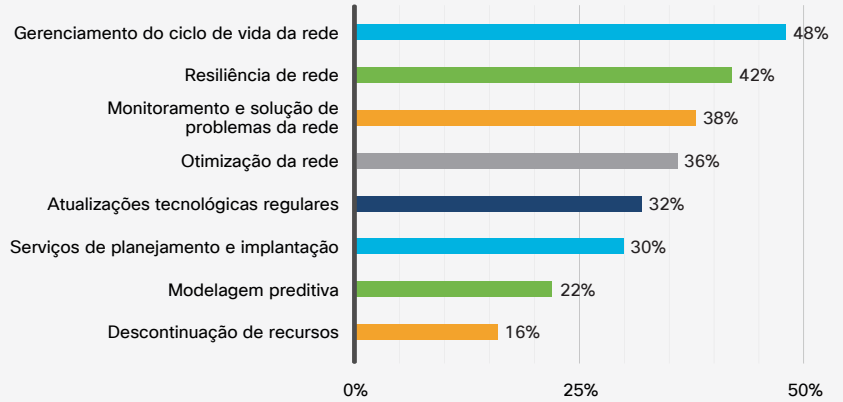
Usando APIs, a equipe de NetOps do cliente também pode gerenciar as integrações entre a NaaS e os sistemas atuais para otimizar os fluxos de trabalho e processos de TI. E provavelmente eles vão querer trabalhar em estreita colaboração com o provedor de NaaS para garantir que os SLAs e os objetivos de nível de serviço (SLOs) sejam atendidos. Independentemente das transferências e responsabilidades operacionais, está claro que os profissionais de TI estão ansiosos para reduzir os encargos do gerenciamento de infraestrutura.



48% dos profissionais de TI entrevistados disseram que o gerenciamento do ciclo de vida da rede é o serviço mais importante a ser incluído em um modelo de NaaS. Resiliência de rede (42%) e monitoramento e solução de problemas de rede (38%) completam os três primeiros. Isso reforça a noção de que o gerenciamento de uma combinação cada vez mais distribuída e complexa de locais, usuários, dispositivos, aplicações e recursos de nuvem deixa muito pouco tempo para atividades de valor agregado e inovação.



Na sua opinião, qual dos seguintes serviços seria mais importante incluir em um modelo de NaaS?



"O provedor lida com os pormenores do dia a dia. Então, a equipe interna pode se concentrar em agregar mais valor por meio da rede, atendendo aos novos requisitos que surgirem. Nossos engenheiros e técnicos não precisam parar para resolver problemas. Eles podem se concentrar em novos projetos."

– Engenheiro de rede sênior, empresa de consultoria global



Resultado:

As responsabilidades operacionais são compartilhadas em um modelo de NaaS. A sobrecarga do gerenciamento do ciclo de vida da rede é transferida para o provedor, permitindo que a equipe de TI do cliente se concentre mais nas atividades operacionais que contribuem com o valor comercial.



Funções, responsabilidades e conjuntos de habilidades

Ao transferir as responsabilidades de manutenção da infraestrutura e gerenciamento do ciclo de vida para o provedor, a NaaS libera bastante tempo. E permite que a equipe de NetOps do cliente se concentre nos resultados de rede desejados, em vez dos aspectos tecnológicos e operacionais de manutenção da infraestrutura.

Em outras palavras, os engenheiros de rede mudam de "pilotar a aeronave" para "comandar a torre de controle". Mas quais tipos de decisões eles esperam tomar?

Segundo nossos entrevistados, 27% acreditam que a equipe de TI aproveitaria o conhecimento técnico - e um painel de NaaS - para converter as necessidades comerciais em políticas de rede. Surpreendentemente, 73% dos entrevistados disseram que prefeririam que fornecedores de terceiros realizassem essa função essencial para os negócios, possivelmente indicando uma percepção de escassez ou falta de confiança nos conjuntos de habilidades internas.

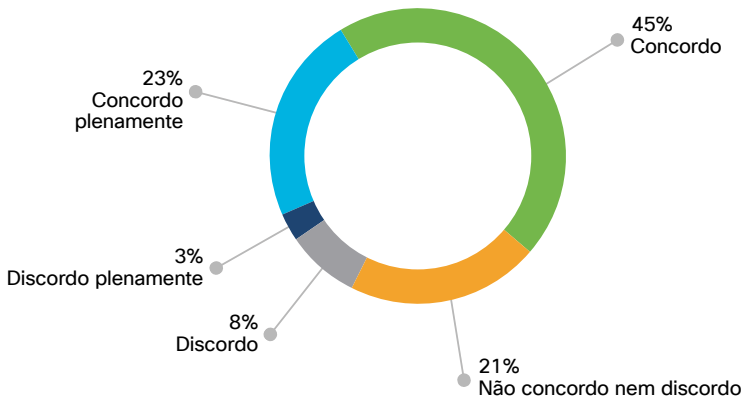
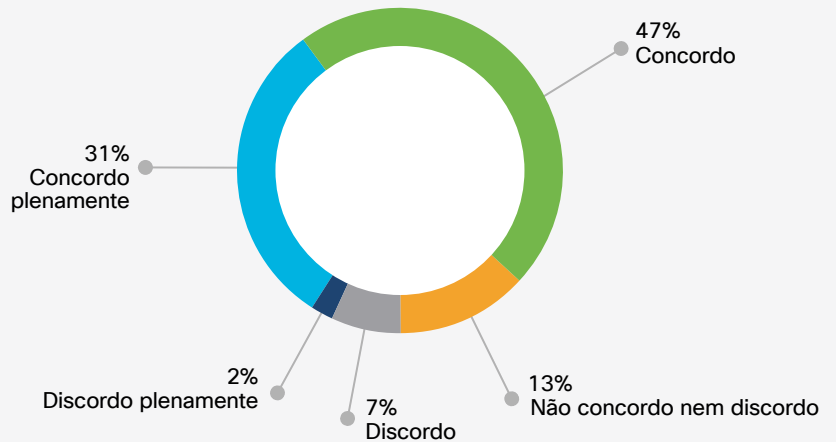


“Com a mudança da maior parte do trabalho diário para o provedor de NaaS, a equipe de NetOps do cliente provavelmente se concentrará nas habilidades gerais de rede e segurança de rede, bem como nas habilidades de design que convertam a intenção dos negócios em conceitos de rede de alto nível. Eles precisarão trabalhar em estreita colaboração com o provedor de NaaS para otimizar projetos, políticas, desempenho e SLAs de rede. E habilidades robustas de ciência de dados serão necessárias para identificar e orquestrar essas mudanças.”

– Joe Clarke, engenheiro distinto, Cisco



A adoção de um modelo de NaaS proporcionaria aos membros da equipe de nossa rede oportunidades de aprimorar as qualificações e agregar maior valor à empresa.



A NaaS liberará minha equipe de rede para se concentrar em tarefas que oferecem inovação em TI e valor comercial, em vez do gerenciamento de rede cotidiano.



Resultado:

Mais de 75% das empresas concordam ou concordam plenamente que os modelos de NaaS darão às equipes uma oportunidade de aprimorar suas habilidades e agregar maior valor.



Preocupações e hesitações

A NaaS impacta muitas áreas de uma empresa de TI, o que exige novos modelos operacionais, novas integrações com processos e tecnologias atuais, mudança de funções e habilidades, além de uma mudança financeira de CapEx para OpEx. Pensando nessas implicações abrangentes, os profissionais de TI com quem falamos tiveram reações variadas à NaaS. E a maioria estava em extremos opostos do espectro, com muitas e poucas adesões à NaaS.

As perspectivas dos líderes de TI sobre a NaaS pareciam refletir sua filosofia de rede global. E essas filosofias foram divididas principalmente em dois campos: "TI de

controle" e "TI enxuta". Os que seguem a filosofia anterior não têm apenas uma equipe altamente qualificada, mas também uma forte crença de que suas equipes devem possuir e controlar totalmente a pilha de rede. Por outro lado, o último grupo está procurando consolidar a TI, reavaliar tarefas rotineiras versus tarefas de valor agregado e encontrar maneiras de transferir a manutenção de infraestrutura. Como esperado, as empresas com uma mentalidade de "TI enxuta" que já transferiram alguns de seus recursos de TI para a nuvem estão muito abertas às soluções de NaaS.

“Estamos nos arrastando com a NaaS porque sentimos que a rede não receberia o cuidado e a priorização que merece e não seria uma combinação perfeita para o nosso ambiente.

– Gerente de TI, rede, agência militar dos EUA

Alguns líderes de TI com quem conversamos mencionaram que suas redes e processos possuem alta exclusividade e não acreditavam que a NaaS pudesse resolver suas complexidades e desafios únicos.

Outros expressaram uma preocupação real de que a NaaS causaria uma mudança em sua empresa de TI.

Embora os líderes de TI compartilhem um amplo conjunto de preocupações, a percepção da perda de controle é a principal. 30% dos entrevistados questionaram se serão capazes de atender às demandas futuras caso adotem a NaaS. Outros entrevistados estavam preocupados com a perda de controle da segurança (26%) e do desempenho (20%). Na verdade, a NaaS foi criada para proporcionar maior escalabilidade sob demanda e suporte mais rápido para as tecnologias mais recentes. E as decisões de segurança, de desempenho e outras decisões de controle importantes ainda dependem da equipe de TI, não do fornecedor de NaaS.

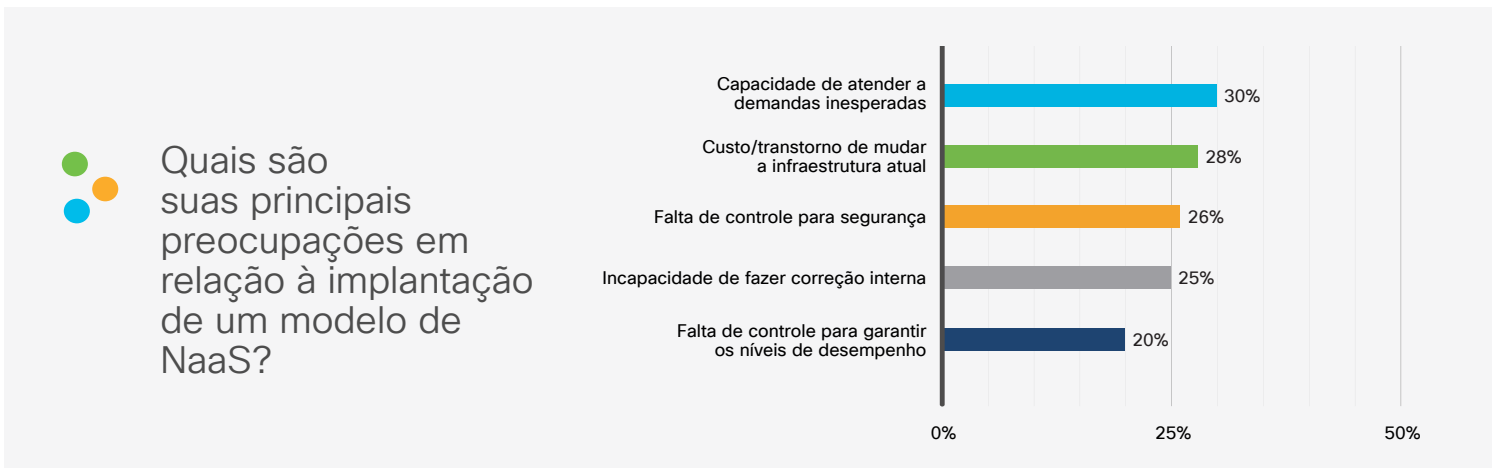




"Um provedor deve se adaptar às nossas diretrizes de segurança e receber nossas orientações. Esse é o principal diferencial da NaaS."

– Arquiteto líder, empresa global de tecnologia

28% dos entrevistados disseram que o custo e a interrupção associados à mudança da infraestrutura e das operações atuais eram inibidores. É compreensível que as empresas tenham uma infinidade de tecnologias e investimentos, dentre os quais, muitos se enquadram em cronogramas de depreciação diferentes. Outras empresas têm tecnologias e aplicações antigas que podem não ser adequados para a NaaS. E algumas simplesmente não querem transferir o gerenciamento cotidiano de sua infraestrutura.



Para resolver essas preocupações e hesitações, as empresas podem começar aos poucos, com um domínio para testar o modelo de NaaS. Isso permitiria que elas entendessem melhor os recursos e os pontos de controle da NaaS, sem alterar muito a infraestrutura ou as operações de rede. Elas poderiam experimentar e otimizar a divisão de responsabilidades entre o provedor e a equipe interna, além de aprender a trabalhar em conjunto para alcançar os melhores resultados. Uma vez que tenham uma compreensão total das funções, responsabilidades e pontos de controle (e se sintam à vontade com isso), elas podem se adaptar e expandir para outros domínios ao longo do tempo, aproveitando os insights e as melhores práticas aprendidas durante a jornada.

Resultado:
Preocupações são esperadas com qualquer modelo de transformação. Os líderes de TI podem começar aos poucos para avaliar os riscos e recompensas associados à NaaS para ver se é ideal para sua empresa.



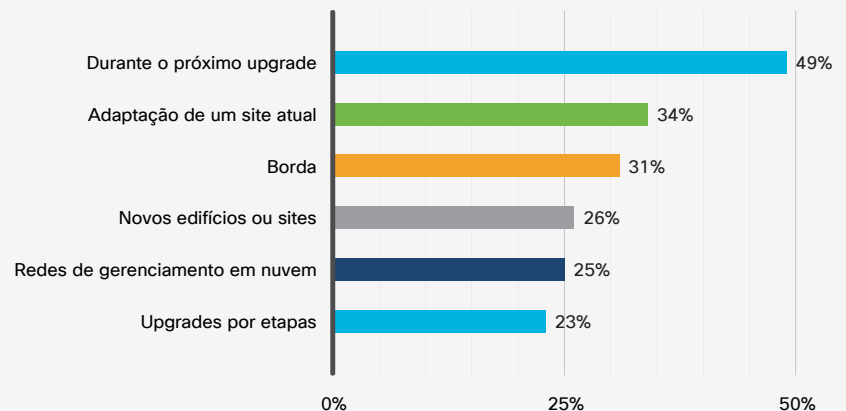
Tendências de adesão

Em virtude de seu impacto nas operações de rede e das diversas maneiras pelas quais pode ser utilizada, a adesão à NaaS será diferente para cada empresa. Uma avaliação de preparação da NaaS e um roadmap de implantação podem minimizar as complicações e maximizar o sucesso.

Segundo nossos entrevistados, 49% dos líderes de TI e 57% dos profissionais de rede acreditam que o melhor momento e circunstância para a adesão à NaaS é durante uma reciclagem ou atualização da infraestrutura de rede, quando procuram acessar uma nova tecnologia (automação, 100 Ethernet Gigabit, Wi-Fi 6, 5G, SD-WAN, SASE etc.). 34% dos entrevistados disseram que a adaptação de um site atual (brownfield) em que a tecnologia de rede já foi implantada é o cenário ideal para a adesão à NaaS. Curiosamente, apenas 26% disseram que um site greenfield seria a melhor opção para a adesão à NaaS. E apenas 23% disseram que uma abordagem em fases, em que os domínios são atualizados um a um com a NaaS, seria o melhor cenário para a sua empresa.



Para qual dos cenários a seguir você acredita que a NaaS seria a melhor opção para a sua empresa?



Resultado:

Como, quando e por que a NaaS é implantada serão diferentes para cada empresa.

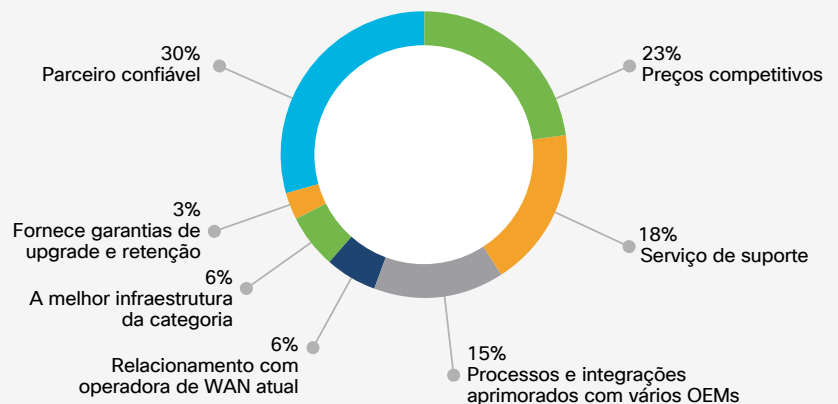


Como escolher um provedor de NaaS

Como a rede é um facilitador essencial da produtividade dos funcionários, do engajamento dos clientes e das operações de negócios, escolher o provedor de NaaS certo não é uma tarefa corriqueira. Alguns dos líderes de TI com quem conversamos têm um medo real de perder o controle. No entanto, eles estão dispostos a desistir de uma medida de controle se, e somente se, o controle for colocado nas mãos de um parceiro confiável. Quer isso signifique trabalhar com um integrador de sistemas, provedor de serviços gerenciados ou revendedor de valor agregado, eles se sentem mais à vontade com parceiros estabelecidos que já têm um conhecimento amplo de seu ambiente de rede, objetivos de negócios e necessidades de suporte.

Para implantações de NaaS, quase um terço dos profissionais de TI em nossa pesquisa considerou os integradores de sistemas mais confiáveis e com preços competitivos, em comparação aos fornecedores de rede. Eles também disseram que a "experiência confiável" era muito mais importante do que "a melhor infraestrutura da categoria".

Qual é o principal motivo pelo qual você prefere trabalhar com um parceiro, em vez de diretamente com um fornecedor de rede para a implantação de NaaS?

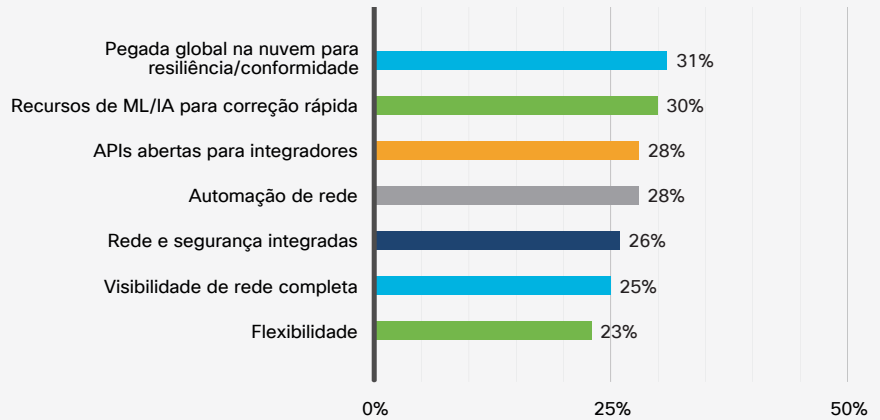


E quando se trata de converter as necessidades comerciais em políticas técnicas, os profissionais de TI são duas a três vezes mais propensos a confiar em um integrador de sistemas ou em sua equipe interna de TI do que em um fornecedor de NaaS. Isso ressalta o fato de que as empresas estão procurando não apenas uma solução, quando se trata de NaaS, mas também a orientação e assistência de um consultor confiável que as conheça bem.

Ao considerar os atributos técnicos das soluções e provedores de NaaS, nossos entrevistados priorizaram uma presença global na nuvem para confiabilidade, desempenho e conformidade regional (31%), bem como recursos de aprendizado de máquina (ML) e inteligência artificial que permitam a otimização contínua do serviço de NaaS (30%). APIs, automação, segurança integrada, visibilidade de rede e flexibilidade de rede também tiveram uma classificação elevada.



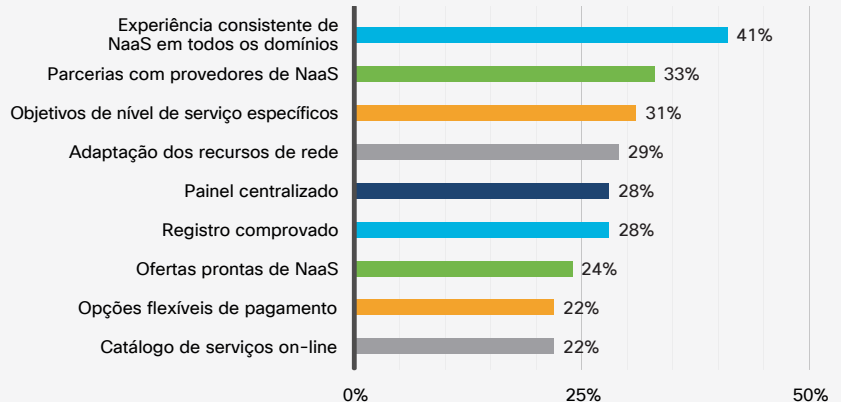
Quais você acredita serem os dois atributos técnicos mais importantes de uma oferta de NaaS?



41% dos entrevistados disseram que é importante que um provedor de NaaS ofereça uma plataforma de NaaS coerente em todos os domínios de rede (acesso, WAN, data center, nuvem etc.). Como muitas equipes de TI têm dificuldades para gerenciar vários ambientes, conjuntos de ferramentas e modelos operacionais, a NaaS oferece uma oportunidade de consolidar recursos, políticas e operações de rede.



Qual das opções a seguir seria mais importante, se você considerasse a oferta de um provedor de NaaS?



"O que estou procurando de fato é alguém que possa lidar com as atividades de gerenciamento de rotina em nossa rede e sistemas, como atualizações de firmware, configurações e alterações. Então, minha equipe pode se concentrar em melhorias, criações e implementações de estratégia. E talvez obtenha flexibilidade. Talvez este mês eu esteja fazendo um trabalho bem pesado sozinho e então receba ajuda por alguns meses para expandir esse uso e auxiliar no trabalho."

– Vice-presidente de tecnologia e segurança, organização sem fins lucrativos de US\$ 100 milhões



Resultado:

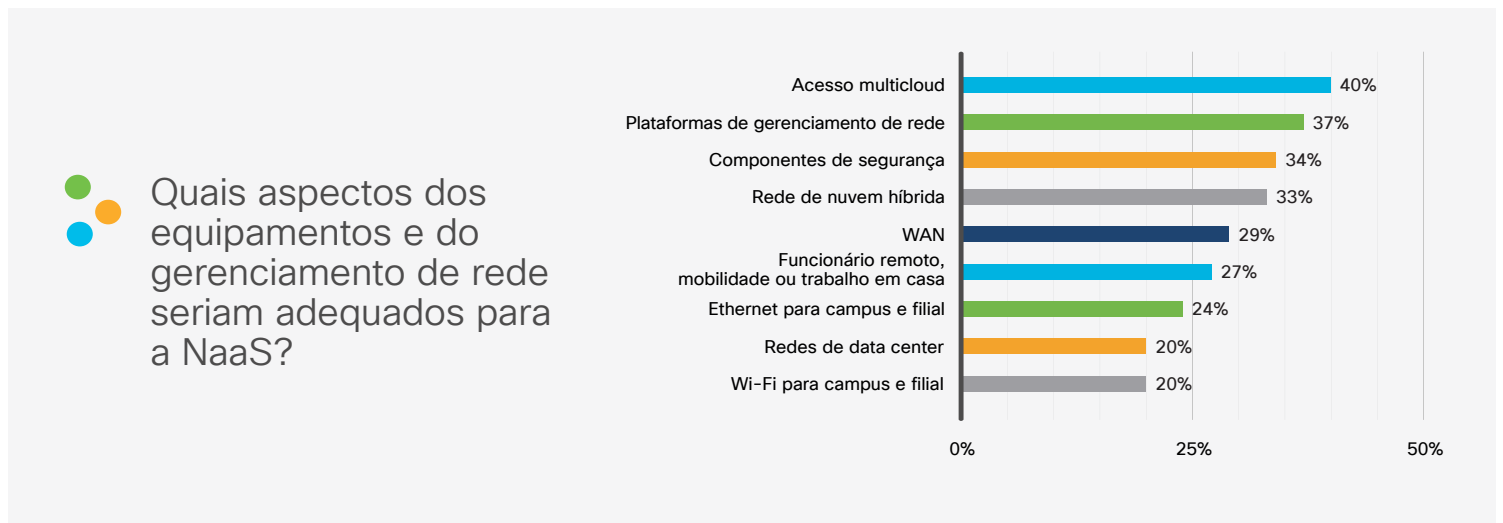
Os integradores de sistemas são considerados mais confiáveis, com preços competitivos e orientados a serviços do que os fornecedores de NaaS. Independentemente do provedor, os clientes procuram um serviço e uma experiência operacional que abranjam todos os domínios da rede.



SASE e as diferentes nuances da NaaS

Há um número crescente de ofertas de NaaS, incluindo LANs com e sem fio, VPNs, WANs, segurança de rede, acesso remoto ou de trabalho em casa, redes de data center e redes em nuvem. De acordo com nossa pesquisa, os modelos de NaaS que incluem acesso multicloud e segurança são os mais desejáveis. Isso significa que a SASE, que fornece acesso multicloud seguro em qualquer lugar, seria uma oferta como serviço sob demanda entre muitas empresas de TI.

Considerando os desafios de se conectar a várias nuvens diferentes, já era esperado que o acesso multicloud fosse identificado como a principal prioridade (40%) para NaaS. Ao oferecer serviços de SD-WAN, os fornecedores de NaaS podem fornecer uma maneira consistente e otimizada de se conectar a uma ampla variedade de aplicações em nuvem (IaaS e SaaS).



34% dos entrevistados priorizaram soluções de NaaS com foco em segurança, incluindo VPN, informações de segurança e gerenciamento de eventos (SIEM), gateway de Web seguro, firewalls e serviços de prevenção e detecção de invasão (IPS/IDS). Isso pode ajudar a proteger usuários, dispositivos e aplicações constantemente em várias nuvens e ambientes de computação.

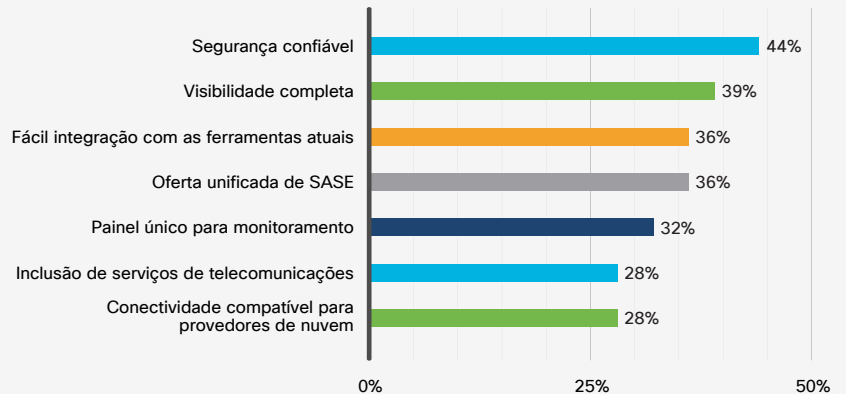
Os fornecedores de NaaS que oferecem uma combinação de acesso multicloud e segurança na borda estão bem posicionados para atender à crescente demanda de soluções de SASE.



Quase metade (44%) dos entrevistados citou “segurança estável, incluindo detecção e correção de ameaças, para todos os usuários e dispositivos”, independentemente do local de acesso, como um aspecto importante da SASE. Com a crescente dependência da Internet para acesso a aplicações em nuvem, mais de uma a cada três (39%) está buscando “visibilidade e insights sobre o tráfego de rede na Internet e nas infraestruturas de nuvem”. E 36% estão procurando soluções de SASE que possam ser facilmente integradas às ferramentas atuais.



Se a sua empresa decidisse implantar a SASE como serviço, qual das opções a seguir você consideraria os recursos mais importantes?



Resultado:

O acesso multicloud e a segurança são as principais prioridades da NaaS. Os fornecedores que incluem uma opção de SASE no portfólio de NaaS podem atender à demanda crescente de alinhamento e proteção dos recursos locais e na nuvem.



Conclusão

Inúmeras empresas de TI têm dificuldades de gerenciar a complexidade da rede, responder a interrupções, proteger usuários e dados e acompanhar o ritmo acelerado dos negócios. Para enfrentar esses desafios, muitas estão investigando novos modelos de rede, como a NaaS.

A NaaS fornece acesso contínuo às tecnologias de rede mais recentes por meio de um modelo sob demanda ou baseado em assinatura. E transfere a responsabilidade do gerenciamento de rede cotidiano para um provedor de terceiros. Ao fazer isso, permite que as equipes de TI se concentrem em atividades de valor agregado que promovem maior agilidade, resiliência e inovação para a empresa.

Como acontece com qualquer modelo transformador, há preocupações e hesitações a respeito da NaaS. Mas não se trata de uma proposta de tudo ou nada. As equipes de TI podem trabalhar com parceiros confiáveis para experimentar a NaaS em pequena escala, avaliar os riscos e recompensas e ver se ela está de acordo com suas estratégias globais de negócios e de tecnologia.



Recursos adicionais e assistência

[O que é rede como serviço \(NaaS\)? >](#)

[Mais soluções da Cisco >](#)

[Localizar um parceiro da Cisco >](#)

[Fale com a equipe de vendas da Cisco >](#)

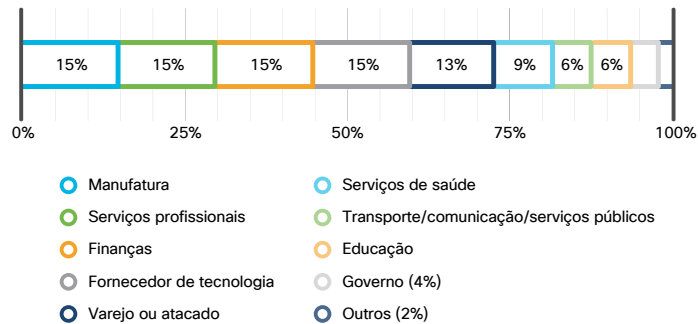


Sobre este relatório

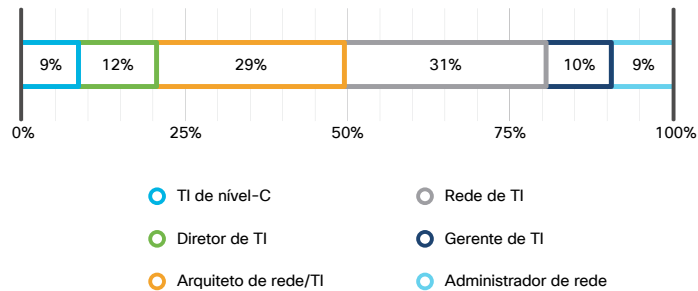
Publicado pela primeira vez em 2019, o [relatório de tendências globais de rede](#) destaca as estratégias e tecnologias mais recentes no segmento de rede empresarial e de nuvem. O relatório aproveita a pesquisa do setor e fornece perspectivas, insights e orientação para ajudar as empresas de TI a entender as tendências atuais de tecnologia, desenvolver os modelos de rede e oferecer suporte às necessidades comerciais dinâmicas.

Para o relatório de 2022, realizamos entrevistas com 20 líderes de TI e recebemos comentários de 1.534 profissionais de TI em 13 países sobre as perspectivas deles em relação à NaaS e como eles veem isso se alinhando ou aumentando suas estratégias de rede nos próximos dois anos. Os entrevistados podiam selecionar até três respostas por pergunta.

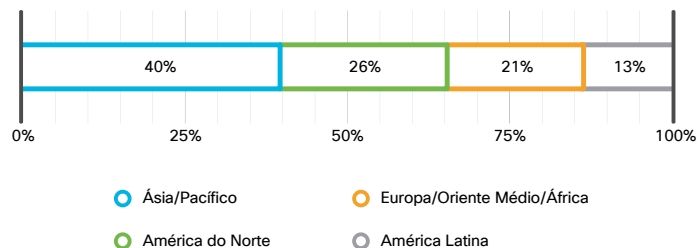
Setor do entrevistado



Função do entrevistado



Localização do entrevistado





Permissões para usar este relatório

A Cisco dá as boas-vindas a todos e incentiva a imprensa, analistas, provedores de serviços e outras partes interessadas a usar as informações contidas neste relatório. Exigimos a devida atribuição de todo e qualquer dado do Relatório da Cisco de tendências globais de rede de 2022 que sejam publicados ou compartilhados – de forma privada ou pública – em formato impresso ou eletrônico (ou seja, “Fonte: Relatório da Cisco de Tendências Globais de Rede de 2022”). Nenhuma outra assinatura e consentimento é necessário para consultar nossos white papers, relatórios ou ferramentas na Web disponíveis ao público.

Estamos sempre atentos ao contexto em que nosso conteúdo é usado. Agradecemos quando as partes que usam nosso conteúdo compartilham cópias de seus trabalhos concluídos contendo inserções do Relatório da Cisco de tendências globais de rede de 2022. Você pode encaminhar documentos contendo referências do Relatório da Cisco de tendências globais de rede de 2022 para networkingtrends-inquiries@cisco.com.

© 2022 Cisco e/ou suas afiliadas. Todos os direitos reservados. Cisco e o logotipo da Cisco são marcas comerciais ou marcas comerciais registradas da Cisco e/ou de suas afiliadas nos EUA e em outros países. Para visualizar uma lista das marcas comerciais da Cisco, consulte a [página de marcas comerciais](#) no site da Cisco. Todas as marcas de terceiros citadas pertencem a seus respectivos detentores. O uso do termo “parceiro” não implica uma relação de sociedade entre a Cisco e qualquer outra empresa. (2205R)

Fontes de tendências globais de rede para 2022

1. Global Network-as-a-Service (NaaS) Market Industry Dynamics, Market Size, and Opportunity Forecast to 2027, março de 2021.