



Sua jornada para o SASE

Garantia de segurança em todos os lugares através do Secure Access Service Edge



Business
Services



Resumo executivo

Os requisitos de TI empresarial são amplos e ambiciosos. A maioria busca maior flexibilidade, experiência de usuário aprimorada, otimização organizacional e a capacidade de gerenciar uma força de trabalho cada vez mais distribuída. Provavelmente você já ouviu dizer que o Secure Access Service Edge - SASE promete entregar tudo isso. O que você talvez não perceba é que você já está na jornada SASE.

A maioria das empresas estão na fase inicial da transformação SASE. À medida que avançamos, todas as empresas que adotaram o SD-WAN para fornecer serviços baseados em nuvem devem levar o SASE adiante. No entanto, é essencial observar que o SASE se trata da aquisição de uma metodologia, não de uma plataforma. Trata-se de pequenos passos para a visão do todo e, em seguida, começar com um desafio maior, como o acesso remoto e de criar uma ponte para o SASE.

Neste artigo, a Orange Business Services se une à Palo Alto Networks para refletir sobre o que o SASE traz para as empresas e como elas podem acelerar sua jornada SASE através desta parceria. Também examinamos como as empresas podem implementar uma estratégia SASE proativa que visa resultados de negócios individuais, identificando dependências e prioridades que conduzirão ao sucesso.

Continue lendo para saber como se beneficiar do SASE em sua organização.

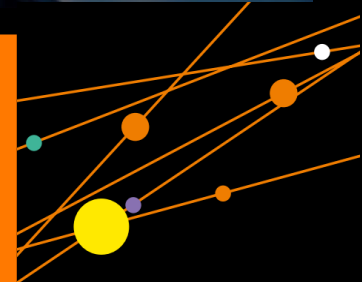
60%

Até 2025, pelo menos 60% das empresas terão estratégias e prazos para a adoção do SASE, abrangendo usuário, setor e acesso ao edge, a partir de 10% em 2020.¹



Índice

Resumo executivo	2
Por que o SASE?	3
A jornada para o SASE	
O SASE apoia os negócios digitais	6
Passos estratégicos para substituir seu patrimônio legado	8
A abordagem Orange ao SASE	9
Por que a Orange?	10

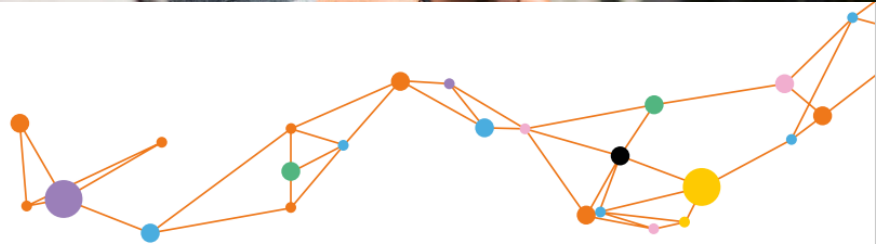


Por que o SASE?

O “cloud-first” está rapidamente se tornando a norma para as empresas, e o processamento está se afastando do data center para a fronteira da rede em algumas cargas de trabalho, mas não necessariamente para todas, exigindo integração do cloud-first com cargas de trabalho que não necessariamente se prestam à migração para nuvem. Os usuários precisam de acesso imediato e ininterrupto aos dados e aplicações onde quer que estejam trabalhando. O grande desafio neste ambiente cada vez mais dinâmico e em expansão é manter tudo isso em segurança.

O SASE pode ser a resposta? Uma estratégia emergente de segurança cibernética e rede orientada para a nuvem converge serviços de rede e segurança para proteger os usuários, aplicativos e dados. Uma arquitetura SASE identifica dispositivos e usuários, aplica uma segurança consistente baseada em políticas e fornece acesso seguro a aplicações ou dados apropriados.

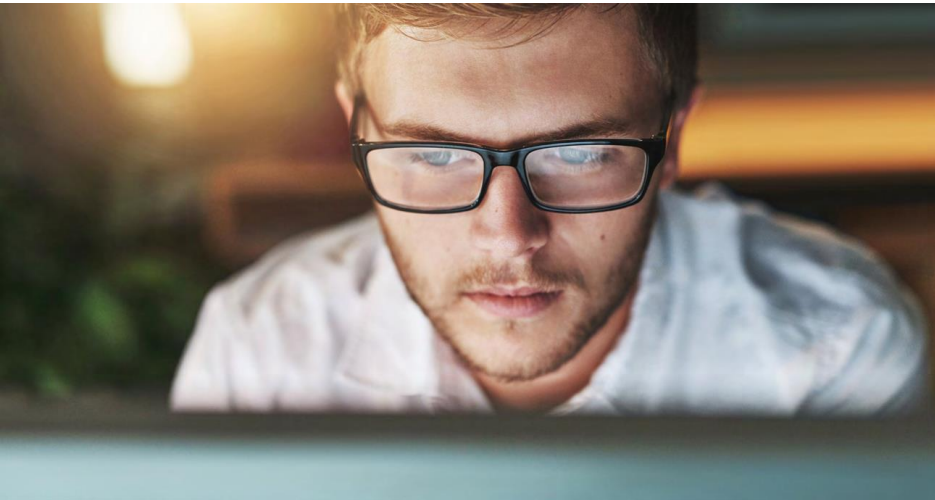
Fundamentalmente, o SASE combina as capacidades de Software-defined Wide Area Network (SD-WAN) com um conjunto de estratégias de segurança prescritivas orientadas em torno da segurança dos ativos, significativamente à medida que a tecnologia de nuvem "como serviço" acelera. Esta abordagem de segurança oferece rede e serviços de segurança em nível de sub e sobreposição como um serviço único, reduzindo a complexidade. Ela converge a melhor segurança e os recursos SD-WAN para proporcionar uma experiência única ao usuário, ao mesmo tempo em que reduz os riscos à segurança.



A jornada para o SASE

Conforme as empresas migram para a nuvem, elas percebem rapidamente que a infraestrutura e a segurança da rede não podem mais operar em silos. Muitas organizações já começaram sua jornada SASE, mas às vezes desconhecem onde estão precisamente no processo. Assim, começa abordando seus desafios de transformação digital, computação de ponta e uma força de trabalho dinâmica.

O SASE não é um produto isolado que possa ser adquirido. Em seu mais alto nível, a implantação de uma arquitetura SASE é construída em torno da ideia de permitir conectividade segura e acesso a recursos do perímetro. Para funcionar de forma eficiente, todos os componentes do modelo de conectividade SASE, rede e segurança, precisam se integrar perfeitamente como parte de um sistema gerenciado de forma centralizada.

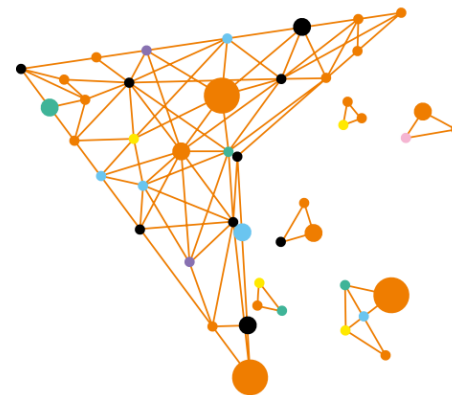


Não há uma solução pronta para o SASE

O caminho para o SASE está longe de ser simples. Toda empresa tem seu ponto de partida, o que requer reflexões, flexibilidade e customização.

A jornada SASE proporciona maior flexibilidade e proteção de dados, redução da complexidade e maior desempenho - proporcionando ganhos em produtividade e lucratividade. Ao invés de comprar e gerenciar produtos de múltiplos pontos, uma única plataforma aumentará significativamente a eficiência dos recursos de TI e oferecerá à empresa maior agilidade, trazendo rede e segurança em uma única tela.

Até 2023, para fornecer largura de banda flexível, econômica e escalável, 30% das localidades empresariais terão apenas conectividade WAN pela Internet, em comparação com aproximadamente 15% em 2020.²



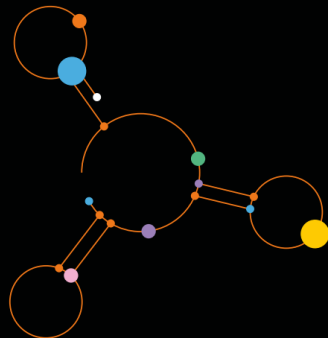
Habilitando o Zero Trust

Zero Trust Network Access (ZTNA) é um componente essencial na arquitetura SASE, essencial para oferecer segurança de ponta a ponta. O ZTNA foi projetado para impor uma política de confiança zero construída em torno do conceito de "nunca confiar, sempre verificar". Basicamente, o nível de confiança é fixado em "zero". A inspeção completa do conteúdo integrado ao SASE oferece melhor segurança e visibilidade na rede.

A necessidade de apoiar empreendimentos de transformação digital ágil de negócios com uma postura de segurança de confiança zero enquanto gerencia a complexidade é crucial para a adoção do SASE.³

Juntos, o SASE e o ZTNA podem melhorar significativamente sua postura geral de segurança ao:

- Trazer escalabilidade segura para uma plataforma multi-tenant cloud-native
- Aumentar a granularidade em termos de visibilidade da rede e controle de políticas
- Fornecer segurança sem redução de desempenho
- Proporcionar segurança a todo momento em qualquer lugar funcionando sem impactar a produtividade



60%

Até 2023, junto com o SASE e o ZTNA, 60% das empresas irão eliminar suas VPNs em prol de soluções baseadas no ZTNA.⁴

O SASE apoia negócios digitais

Com a explosão dos negócios digitais, as redes estão se tornando cada vez mais distribuídas e virtualizadas. O SASE pode ajudá-lo a entregar na nuvem e outras aplicações com segurança aos usuários finais.

A transformação digital e rápida adoção da nuvem mudaram a rede empresarial. Mais usuários trabalham remotamente e mais dados confidenciais são mantidos na nuvem e fora do perímetro empresarial tradicional. Ter esse acesso à empresa de qualquer lugar é outro fator que contribui para a adoção do SASE.

A vantagem da arquitetura SASE é que ela incorpora tecnologias fornecidas por assinatura para integrar segurança na rede a qualquer hora e em qualquer lugar de acesso. Assim, a prestação de serviços na nuvem é mais segura e fluida. Pode-se aplicar políticas de segurança consistentes para todos os usuários e ativos independentemente da localização, seja em data centers, na nuvem, ou SaaS - sem qualquer redução de desempenho.

"A grande maioria da adoção do SASE empresarial ocorrerá ao longo de vários anos, priorizando as áreas de maior oportunidade em ganhos de eficiência, eliminando a complexidade e os fornecedores redundantes, e a redução de riscos através da adoção de uma postura de confiança zero." ⁵
Neil McDonald, vice-presidente analista, Gartner.

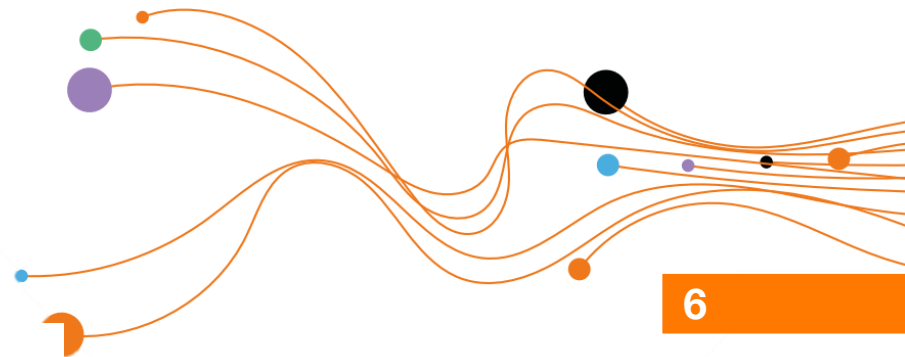
Um processo de transformação

Uma estratégia de infraestrutura SASE não pode ser alcançada da noite para o dia. É um processo de transformação que substituirá as VPNs existentes, firewalls de hardware e dispositivos de proteção DDoS ao longo do tempo.

O SASE fornece um conjunto de funcionalidades que podem ser introduzidas em seu próprio ritmo, permitindo que você adote serviços adequados para as suas necessidades comerciais. Eles normalmente incluem SD-WAN, gateways web seguros (SWG), corretores de segurança de acesso à nuvem (CASB), firewalls de última geração e ZTNA. Uma arquitetura SASE pode coexistir com seu portfólio atual de redes e segurança até que os ativos cheguem ao fim da vida útil ou sejam aposentados.

De acordo com o Gartner, a adoção do SASE será parcialmente impulsionada por ciclos de atualização da rede e da solução de segurança de rede e programas de offload MPLS projetados para tornar o tráfego na nuvem mais eficiente ⁶. Aqui, as conexões diretas à Internet podem ser usadas para descarregar o tráfego destinado à Web, se necessário. Algumas empresas, no entanto, têm políticas que restringem isso.

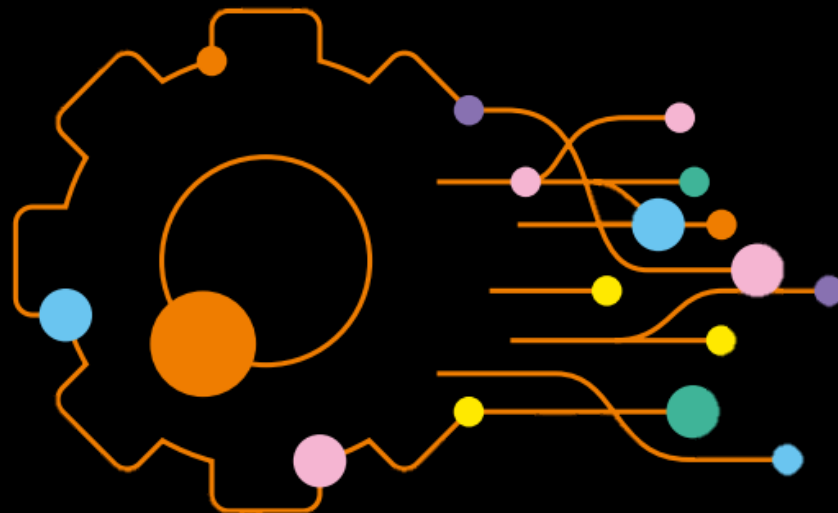
Se você ainda não olhou para o SASE, agora é a hora de criar uma estratégia global para substituir o patrimônio legado por um modelo SASE convergente. Isto é essencial para administrar efetivamente os custos, a complexidade e as demandas de apoio aos negócios em um ambiente dinâmico em evolução.



Benefícios comerciais estratégicos do SASE

Como o trabalho remoto continua a se tornar o “normal” e uma abordagem “cloud-first” continua a crescer, o SASE também traz os seguintes benefícios estratégicos para seu negócio:

- Converte as funcionalidades de rede e segurança em um único serviço fornecido na nuvem, gerenciado a partir de um único console, reduzindo custos e complexidade
- Aplica acesso à rede com privilégios mínimos utilizando o ZTNA, melhorando a postura de segurança
- A aplicação consistente da política de segurança reduz as exigências de recursos, liberando as equipes para se concentrarem em projetos geradores de receita
- A utilização de políticas de identidade e contextuais oferece uma abordagem mais dinâmica e granular de segurança - permitindo que você abra suas portas virtuais aos parceiros de negócios enquanto mitiga os riscos.
- O gerenciamento na nuvem permite que as empresas implementem e escalem serviços rapidamente sem dispositivos adicionais ou conexões com hardwares
- Garante a segurança corporativa e regulatória, não importa onde ou quando os funcionários estão logados
- Traz escalabilidade segura a uma plataforma multi-tenant cloud-native
- Maior granularidade em termos de visibilidade da rede e controle de políticas
- Segurança sem redução de desempenho
- Proporciona segurança a todo momento em qualquer lugar funcionando sem afetar a produtividade



Passos estratégicos para substituir seu patrimônio legado

Uma transformação para uma arquitetura SASE leva tempo. Os investimentos em contratos de hardware e software podem ainda não estarem prontos para substituição.

Para complicar ainda mais o quadro, muitas grandes empresas têm equipes separadas de segurança de rede e operações de rede que operam em silos. O Gartner sugere a criação de equipes unificadas responsáveis pela engenharia de acesso para unificar redes e políticas de rede em toda a organização, da mesma forma que a engenharia de plataforma trabalha com o DevOps.

Entretanto, muitas empresas iniciaram sua jornada SASE (quer saibam ou não) e podem não ter avaliado em que nível estão em sua segurança e em seus guias de rede em relação ao SASE como uma arquitetura de referência. Um primeiro passo essencial para continuar sua jornada SASE é selecionar um parceiro de confiança. Eles podem ajudar na avaliação da tecnologia, estabelecendo provas de valor, ou quais adaptações você pode precisar fazer para integrar componentes específicos do SASE. Isto pode ajudá-lo a construir sua segurança e seus roadmaps de redes.

Além disso, embora muitos fornecedores estejam promovendo soluções SASE, nem todos oferecem as capacidades SASE necessárias. Você deve medir suas exigências em relação às melhores ofertas até que o mercado amadureça e as lacunas sejam fechadas.

Até 2025, pelo menos 60% das empresas terão estratégias e prazos explícitos para a adoção do SASE, abrangendo usuário, filial e acesso edge, a partir de 10% em 2020.⁸

O Gartner⁷ chega a estabelecer um plano de três a cinco anos para a transformação SASE, abrangendo abordagens de acesso seguro para usuários, filiais, localizações de edge e aplicações distribuídas. As mudanças sugeridas incluem:

- **VPN:** Substituir o acesso VPN de nível de rede por acesso de confiança zero. Além disso, adotar ZTNA com base na nuvem para complementar o acesso VPN legado para cenários de maior risco, como o acesso não gerenciado a dispositivos.
- **Demilitarized Zone (DMZ):** iniciar a eliminação gradual dos serviços baseados em DMZ para acesso do usuário designado.
- **Iniciar a substituição dos dispositivos físicos SWG, CASB e VPN** pela nuvem quando houver oportunidades de atualização.
- **Implantar Firewall como Serviço (FWaaS)** que afasta a funcionalidade do firewall do perímetro tradicional da rede para a nuvem.

Roadmap robusto de migração

É importante reiterar que o SASE não é um caso de “ligue e vá”. Requer um roteiro estratégico de migração que cubra as exigências de filial, edge, campus, sede e acesso remoto. O plano de migração deve ser constantemente reavaliado à medida que o mercado SASE amadurece.

O uso de um único fornecedor para segurança de rede como serviço e a consolidação de stacks de tecnologia reduzem os custos e a complexidade. No entanto, duas jornadas SASE não são a mesma. Cada empresa precisará se preparar de maneira diferente e se planejar para resultados diferentes.

Uma coisa que o SASE faz para todas as empresas é alinhar processos e simplificar as redes complicadas e suas operações de segurança. Isso permite redesenhar políticas de rede e criar um modelo que permita negócios seguros na nuvem.

A abordagem Orange ao SASE

O modelo SASE pode levar vários anos para funcionar de forma efetiva. Isso exige uma estratégia SASE bem pensada de longo prazo e identificação de táticas de consolidação SASE de curto prazo.

Nem todas as empresas têm as habilidades, recursos ou tempo para pesquisar, construir, projetar e implementar um modelo SASE. Aqui na Orange Business Services, podemos colocar sua empresa à frente da curva SASE, permitindo que você faça mudanças na rede e na segurança da rede com o mínimo de interrupção - ao mesmo tempo em que capitalizamos os benefícios comerciais.

Podemos fornecer uma avaliação inicial SASE em três etapas:

1. Onde você está em relação ao modelo SASE?
2. Onde você quer chegar? Quais são suas ambições? Quais partes do SASE são metas indispensáveis de adoção? Como funciona sua política de segurança atual dentro de um modelo SASE?
3. Como podemos levá-lo até lá? Em outras palavras, como a Orange pode ajudar você a estabelecer seu guia personalizado SASE.

Podemos planejar a jornada SASE de acordo com suas exigências específicas, assumindo a migração e gerenciando o risco, se necessário. Este é um diferencial crucial quando se trata de nossa oferta SASE.

O SASE exige uma mudança na cultura de TI para adotar uma rede integrada e equipes de segurança. Esta é uma área que muitas vezes é negligenciada. Mas, se as equipes não conseguem sair do trabalho em silos e compartilhar o controle, sua jornada SASE vai atingir alguns obstáculos complicados. Podemos ajudar a garantir que sua jornada

SASE impulse o desempenho e a qualidade organizacional em geral.

Uma oferta única de SASE com a Palo Alto Networks

Nem todas as ofertas de SASE são iguais. O que diferencia nossa abordagem é que ela é construída no Prisma® SASE, uma das soluções SASE mais completas do setor da Palo Alto Networks. Junto com os serviços gerenciados pela Orange Business Services, ela fornece acesso consistente à rede e serviços de segurança para todos os tipos de aplicações através de uma estrutura comum e unificada.

A Orange Business Services e a Palo Alto Networks trazem a interoperabilidade, consultoria, suporte, habilidades de migração e modelos flexíveis de gestão e consumo que as empresas estão exigindo para atingir suas metas SASE.

Esta oferta SASE abrangente fornece:

- Convergência sem compromisso: a melhor segurança da categoria e SD-WAN integrado de forma nativa.
- A melhor segurança da classe: segurança consistente em todas as aplicações, independentemente da localização.
- Experiência excepcional do usuário com visibilidade de ponta a ponta e insights tanto para usuários remotos quanto presenciais.



Por que a Orange?

O SASE é um projeto abrangente e multidisciplinar com muitas peças em movimento. Por isso, é vital trabalhar com um parceiro de confiança que entenda o SASE e possa unir a segurança com sua infraestrutura de rede de forma efetiva.

Na Orange Business Services, oferecemos serviços SASE integrados e, ao mesmo tempo, alavancamos nosso ecossistema ampliado de parceiros de tecnologia de ponta. O aproveitamento das integrações entre ZTNA, CASB, cloud SWG, cloud VPN, FWaaS, SD-WAN, e outras tecnologias heterogêneas será crucial para a concretização de todos os benefícios de uma estratégia SASE.

Diante de uma escassez contínua de habilidades, você também pode entrar em contato com nossa equipe global de profissionais de TI e de segurança, com experiência em otimização de redes, com conhecimento sobre tecnologias novas e emergentes, e familiarizados com medidas regulatórias e de conformidade.

Nossos especialistas em nuvem, segurança e conectividade em todo o mundo podem ajudá-lo em sua jornada SASE. Eles podem apoiá-lo de ponta a ponta, permitindo que você alcance uma estratégia SASE eficaz.



8.900 especialistas na gestão de sua transformação digital



18 Centros de Operações de Segurança (SOCs) ao redor do mundo



2,500 profissionais de segurança em um momento em que o mercado de trabalho para ciber-segurança tem desemprego negativo



A experiência de ponta a ponta garante segurança, desempenho e otimização de custos para sua rede



160 municípios com vendas e apoio local



Nossa equipe de especialistas fornece excelência operacional combinada com ferramentas sólidas para criar um rico catálogo API para melhorar qualquer modelo de cogestão



As capacidades da MSI oferecem simplicidade e gestão simplificada de múltiplos prestadores de serviços

Para saber mais sobre nossa oferta SASE com Palo Alto Networks,

<https://www.orange-business.com/en/partners/palo-alto-networks-prisma-sase-specialized-partner>

Copyright © Orange Business Services 2021. All rights reserved. Orange Business Services is a trading name of the Orange Group and is a trademark of Orange Brand Services Limited. Product information, including specifications, is subject to change without prior notice.



**Business
Services**

Sources:

1. Gartner 2021 roadmap for strategic SASE convergence.
2. Gartner 2021 roadmap for SASE convergence
3. Gartner 2021 roadmap for SASE convergence
4. Gartner Zero trust architecture and solutions 2020
5. Gartner 2021 strategic roadmap for SASE convergence
6. Gartner: e Service Access Secure the Into Converge Security and Edge WAN as Win to How: Trends Market July 2019
7. Gartner 2021 roadmap for strategic SASE convergence
8. Gartner 2021 roadmap for strategic SASE convergence

