Orange
Cyberdefense

SASE: o facilitador de negócios digitais para sua força de trabalho

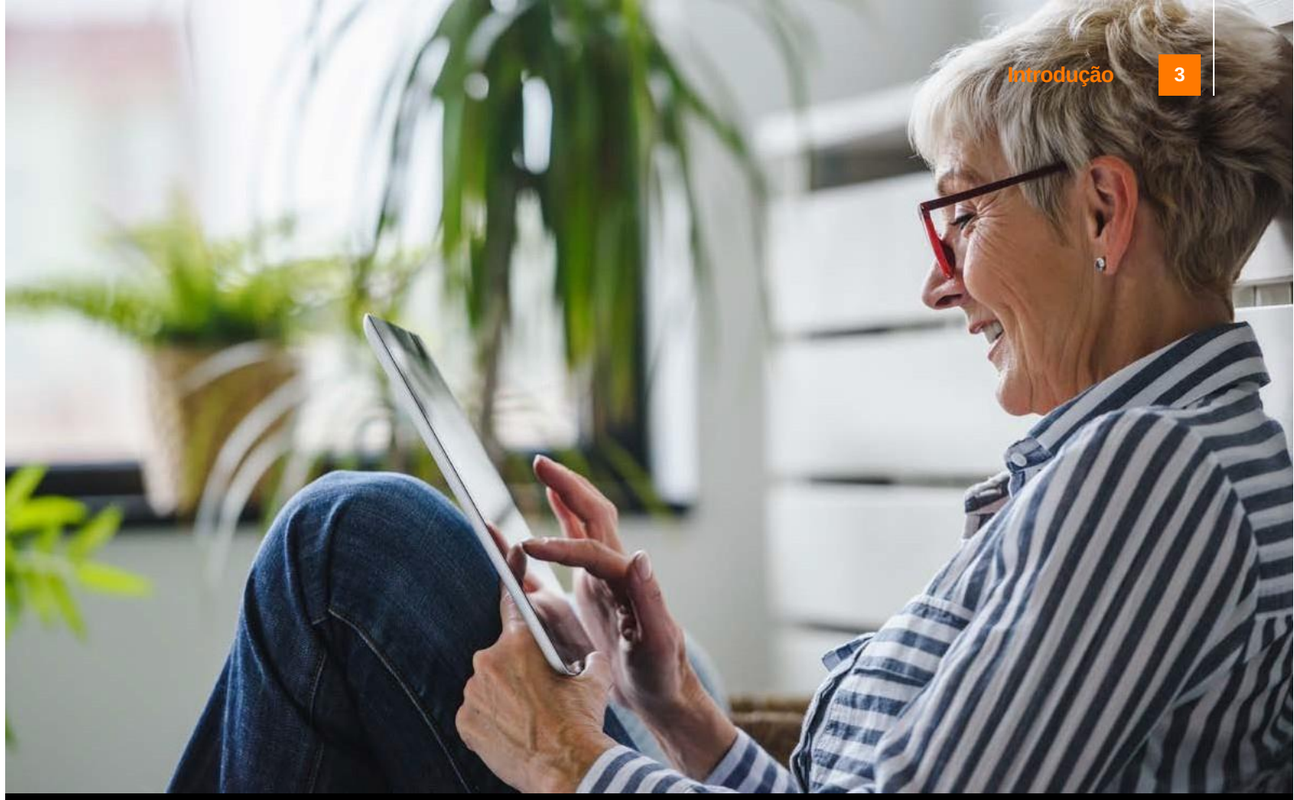
Simplificando sua arquitetura de segurança de rede para o futuro

Simplificando sua arquitetura de segurança de rede para o futuro

Este é um momento de mudança sem precedentes para as organizações à medida que elas transferem seus serviços para a nuvem, e seus funcionários se dispersam mais. Para apoiar este novo modelo, a Internet está se tornando a nova rede corporativa. A tradicional arquitetura de segurança centrada em rede é muito complexa para lidar com este novo paradigma. Ela está se tornando um obstáculo que inibe as necessidades dos negócios digitais. Chegou a hora de uma nova arquitetura de segurança.

Índice

De autoria de: José Araujo, Grupo CTO, Orange Cyberdefense © Orange Cyberdefense, con la apoyo de: Étienne Greeff, Grupo CTO, Orange Cyberdefense y Tomás Surdon, Estrategic Marketing and Innovation Director, Connectivity Business Unit, Orange Business Services



Introdução

O ambiente empresarial moderno exige acesso seguro aos dados e aplicações de qualquer lugar, a qualquer hora, de qualquer dispositivo, onde quer que esses ativos estejam hospedados. O modelo tradicional de segurança de rede não suporta isso adequadamente. O modelo foi construído para dispositivos e usuários que raramente deixavam a rede da empresa. Esses dispositivos eram protegidos por um perímetro rígido que protegia tudo que estava dentro.

Em seguida, usuários, dispositivos e aplicações foram movidos para fora da rede. O modelo baseado em perímetro tornou-se menos relevante à medida que a computação móvel e na nuvem arremessou ativos por toda parte. Precisávamos de algo mais sutil para substituí-lo.

Em agosto de 2019, o Gartner propôs um novo modelo conhecido como o serviço de acesso seguro (secure access service edge - SASE). Ele reestruturou as redes e a arquitetura de segurança de rede para ajudar as empresas a lidar com as mudanças nas exigências de segurança enfrentadas pela empresa dividida em diferentes espaços.

O SASE é uma iniciativa desafiadora e de longo alcance. O mercado ainda está alcançando estas ideias enquanto os fornecedores lutam para oferecer a amplitude e a profundidade de soluções necessárias para apoiar este modelo.

Enquanto esperamos por um melhor suporte dos fornecedores, podemos aproveitar a oportunidade para iniciar a conversa e nos engajarmos onde pudermos, monitorando os desenvolvimentos de mercado relacionados ao SASE e ajudando nossos clientes a construir estratégias de adoção a longo prazo com nossa abordagem orientada pela inteligência.

Este documento de solução explica o modelo SASE e seus benefícios, abordando os desafios atuais.

Ele o guiará enquanto você se prepara para adotar esse modelo e proteger seus negócios digitais e distribuídos.

O que é SASE?

SASE é um mindset, não um produto único. Une rede e segurança de rede, oferecendo acesso seguro a todos os usuários de todos os lugares. Não é simplesmente uma solução que as empresas possam instalar e esquecer. É uma disciplina que precisa de monitoramento contínuo, detecção, e resposta impulsionada pela inteligência de ameaças em constante evolução.

O SASE transfere múltiplas proteções de web, nuvem, dados e ameaças para serviços de segurança que ficam na borda da rede de área ampla (wide-area network), perto dos locais dos usuários. Este modelo depende muito da identidade do usuário ao conceder acesso a dados e aplicações, em vez de confiar em dispositivos ou redes individuais.

Esta nova abordagem redefine o perímetro tradicional, substituindo os sistemas de segurança cibernética locais por serviços integrados à nuvem. Redefine estes serviços de segurança de rede em software, criando uma plataforma única que pode aplicar políticas de segurança unificadas por sessão para um controle de segurança granular.

Este ecossistema unificado de segurança de rede abrange uma rede global, permitindo que os usuários tenham acesso a serviços de forma segura e consistente de qualquer lugar. Também é extensível, permitindo que as empresas ofereçam mais serviços de segurança à medida que as necessidades comerciais evoluem.

Por que precisamos dele?

O SASE representa uma mudança radical na forma como lidamos com a segurança, juntamente com um grande investimento em tempo e esforço. Por que as empresas o implementariam?

Em um mundo onde as práticas e infraestruturas de trabalho estão enfrentando mudanças profundas, as organizações devem encontrar novas maneiras de manter o controle de seus dados. Elas devem suportar uma nova era na qual dispositivos não confiáveis se conectam a recursos de TI distribuídos a partir de redes não controladas.

As organizações precisam do SASE para lidar com a complexidade extra que isso cria. Ele oferece uma infraestrutura integrada de rede e segurança de rede para gerenciar o desempenho e a segurança a partir de um único ponto, utilizando uma política programável unificada. A transformação das nuvens é um fator importante para o modelo SASE.

> “ A IDC prevê que os gastos totais mundiais com produtos e serviços na nuvem sustentarão uma taxa de crescimento anual composta de **15,7%** (CAGR) até 2024.[1]

Os serviços de segurança devem proteger as aplicações e os dados para onde quer que eles vão, e eles vão cada vez mais para a nuvem. A IDC prevê que os gastos totais mundiais com produtos e serviços na nuvem sustentarão uma taxa de crescimento anual composta de 15,7% (CAGR) até 2024.1 A nova abordagem do SASE para a segurança de rede será cada vez mais importante à medida que mais aplicações se tornarem nativas da nuvem.

> “ Os números da Comissão Europeia constatam que cerca de **40%** dos trabalhadores da UE mudaram para o home office em tempo integral durante a pandemia da COVID-19. [2]

O SASE também se torna mais necessário à medida que nossos padrões de trabalho mudam. A pandemia acelerou uma tendência crescente de trabalho em home office, com os números da Comissão Europeia descobrindo que cerca de 40% dos trabalhadores na UE mudaram para o home office em tempo integral durante a pandemia da COVID-19. Isso é um aumento maciço, dado que apenas 15% dos trabalhadores da UE já haviam aderido antes da crise.

Em apenas alguns meses, já vimos lacunas na segurança do perímetro tradicional, à medida que as empresas lutam para servir uma nova e remota força de trabalho. Por exemplo, o National Cyber Security Centre do Reino Unido e a US Cybersecurity and Infrastructure Security Agency (CISA) emitiu uma assessoria conjunta em abril de 2020, no início do alerta de pandemia de vários ataques relacionados à COVID-19, visando a infraestrutura de acesso remoto e contas de trabalhadores remotos. [3]

Em um mundo pós-pandêmico, as pessoas são o novo perímetro. Os trabalhadores remotos precisam de acesso mais rápido, simples e seguro às suas aplicações, mesmo quando não utilizam dispositivos confiáveis. SASE é a chave para esse acesso seguro.

O crescimento da IoT também está criando uma necessidade para o modelo SASE. De acordo com a IDC, até 2025, haverá 55 bilhões de dispositivos conectados em todo o mundo, 75% dos quais se conectarão a uma plataforma IoT. 4 Isso cria uma grande quantidade de dados, que as organizações devem tratar com segurança. O volume de dados da Internet de alta velocidade aumentará para 73 zettabytes em 2025 de 18 zettabytes em 2019, a empresa analista advertiu.

Esta categoria em rápido crescimento está acelerando o acesso à borda para uma enchente de novos dispositivos desafiadores. Uma mistura de grandes volumes de dispositivos e equipamentos com pequenas pegadas de energia e memória torna a segurança do terminal IoT um desafio a ser implementado. A transferência da segurança para a borda da nuvem ajuda a resolver esses problemas de volume e complexidade da infraestrutura.

Benefícios

O SASE fornecerá um rico conjunto de serviços de segurança de rede de forma consistente e integrada para apoiar a transformação dos negócios digitais, computação de ponta e mobilidade da força de trabalho. A adoção do SASE trará os seguintes benefícios:

Flexibilidade
O SASE permite que as organizações direcionem o tráfego para a nuvem de qualquer lugar em vez de encaminhá-lo através do centro de dados, eliminando um grande congestionamento de dados.

Economia de custos
Colocar a segurança da rede na nuvem ajuda a reduzir os gastos de capital para a infraestrutura no local. As empresas que adotam um modelo SASE desfrutarão de gastos operacionais previsíveis a partir de um modelo de segurança baseado em serviços.

Complexidade reduzida
As organizações podem mudar a equipe de segurança do gerenciamento de dispositivos individuais para a entrega de serviços de segurança baseados em políticas a partir de um único ponto, permitindo que configurem redes de ponta a ponta e estruturas de segurança de rede de forma mais simples e coerente.

Aumento da automação
A infraestrutura definida por software é um princípio fundamental da proposta SASE. Ela cria uma plataforma tecnológica convergente que suporta a aplicação de políticas unificadas de forma programática. Assim como os desenvolvedores de software apreciaram o DevOps, os administradores podem desfrutar de um modelo automatizado de operações de segurança de ponta a ponta.

Melhor desempenho
O SASE melhora e acelera o acesso aos recursos da Internet através de uma infraestrutura de rede global otimizada para baixa latência, alta capacidade e alta disponibilidade.

Confiança zero
A confiança zero está no cerne do modelo operacional SASE. Ele oferece acesso seguro a aplicações privadas em nuvens e centros de dados públicos, em vez de acesso em nível de rede.

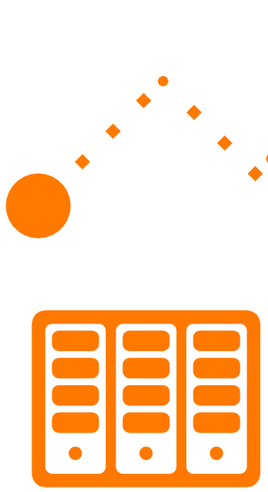
Proteção contra ameaças
Al poner la seguridad en el Ao colocar a segurança na borda da rede entre o usuário e a nuvem, o SASE permite que as empresas detectem e previnam melhor ataques como phishing na nuvem, malware, ransomware e infiltrados maliciosos.

Proteção de dados
Ao concentrar a proteção na identidade, o SASE oferece proteção no nível dos dados, concedendo às pessoas acesso aos principais ativos de dados em uma base de privilégios mínimos como parte de um rigoroso processo de verificação de identidade. Assim, os dados são protegidos em qualquer lugar, desde dentro da organização até a nuvem pública, em redes não confiáveis, e muito além.

A proposta de arquitetura SASE

Durante anos, as redes conectaram os usuários a aplicações no data center. Estes perímetros de rede utilizavam múltiplos controles de segurança para proteger aplicações e dados de interferências externas. As organizações às vezes adicionavam segmentação para limitar o efeito de uma violação do perímetro, juntamente com dispositivos avançados de segurança dentro do perímetro para adicionar camadas extras de proteção.

No início, as redes de área ampla (wide-area networks) que ligavam os usuários aos data centers usavam linhas lentas, caras e dedicadas. Então, várias coisas aconteceram em conjunto: as aplicações migraram para a nuvem, as redes de borda se tornaram mais predominantes à medida que a tecnologia IoT evoluiu, e o mundo mudou para conexões de internet mais rápidas e baratas. Mais recentemente, os usuários aumentaram essas pressões, deslocando-se para fora do perímetro de forma mais permanente à medida que os padrões de trabalho foram mudando.



1

O problema com a arquitetura atual

Este modelo de segurança de rede baseado no perímetro não pode mais suportar o novo contexto. Na verdade, ele acrescenta complexidade e custo. Ele ainda força as conexões através do data center mesmo para aplicações na nuvem, o que transforma o data center em um obstáculo caro.

Os dispositivos de segurança cibernética no centro de dados são inflexíveis. Eles dependem da localização, dependem do tráfego que passa por uma rede específica, e não são facilmente escalonáveis. Raramente utilizam uma camada de controle definida por software, o que os torna complexos de configurar e difíceis de integrar. Isso torna difícil aplicar e manter uma segurança consistente, criando lacunas na postura de segurança.

Embora este modelo possa ter funcionado para funcionários vinculados ao escritório, devemos repensá-lo em um ambiente pandêmico que coloca a maioria dos funcionários fora desses controles de segurança tradicionais. Devemos reavaliar nossos planos de resposta a incidentes e reavaliar a responsabilidade pela segurança neste novo ambiente de trabalho.

2

Como o SASE nos faz avançar

Em um moderno negócio digital centrado nas nuvens, os usuários e dispositivos estão em todos os lugares, assim como os recursos que eles precisam acessar. Também precisamos de serviços de acesso seguro em todos os lugares, integrados em uma rede global que esteja pronta para servir os usuários onde quer que eles estejam.

Neste tecido mundial, os serviços de segurança baseados em containers funcionam na nuvem em pontos de presença (POPs) baseados em bordas. Estes serviços incluem firewalls, gateways web seguros (SWGs), corretores de segurança de acesso à nuvem (CASBs), acesso à rede de confiança zero (ZTNA), DNS seguro, DHCP, e gerenciamento de endereços IP (DDI).

O SASE se baseia nestes serviços definidos por software com características de segurança adicionais que oferecem proteção de ponta a ponta da rede. Assim, os dados ficam protegidos durante todo o seu percurso desde o usuário até a aplicação, independentemente da localização.

Neste modelo, as rotas de tráfego se baseiam dinamicamente nos requisitos da sessão. Ele permite o acesso direto às aplicações de nuvem sem roteamento através do centro de dados, o que reduz a latência e a carga de recursos corporativos, ao mesmo tempo em que reforça a segurança.

Este modelo de segurança baseado em bordas coloca os serviços de segurança cibernética mais próximos dos ativos que eles estão protegendo. Esses ativos podem ser filiais, mas também podem ser usuários individuais ou até mesmo dispositivos IoT. A segurança de rede baseada em bordas suporta todos eles.

A identidade é a chave para a autenticação neste modelo de acesso à rede de confiança zero. Em vez de depender de dispositivos confiáveis para a autenticação, estes serviços de segurança cibernética baseados na borda se concentram na identidade de qualquer coisa que esteja fazendo a conexão.

Esta abordagem protege os usuários em redes domésticas e públicas inseguras, não apenas as corporativas. Os usuários que acessam o SASE a partir de redes domésticas normalmente usariam em seu dispositivo um agente de gerenciamento de endpoints que o protegeria de ataques e potencialmente protegeria os dados da empresa de ativos particulares. Entretanto, é possível suportar dispositivos totalmente não gerenciados, encaminhando-os para ambientes sandboxed via POP.

> “ A identidade é chave para a autenticação neste modelo de acesso à rede de confiança zero. Em vez de depender de dispositivos confiáveis para a autenticação, estes serviços de segurança cibernética baseados na borda se concentram na identidade de qualquer coisa que esteja fazendo a conexão.

No entanto, trabalhar em casa envolve mudanças culturais mais amplas que exigem camadas adicionais de segurança. As redes domésticas abrigam dispositivos não confiáveis, como PCs domésticos e smart TVs. As arquiteturas de segurança devem reconhecê-los.

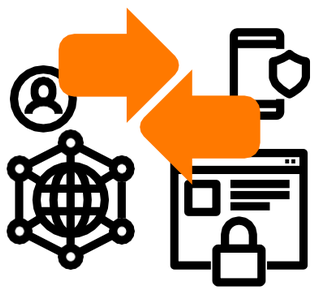
As organizações devem considerar o que compreende a rede corporativa em um mundo de trabalho remoto. As casas dos funcionários são uma extensão da rede corporativa? Os empregadores devem tratar as ameaças no ambiente doméstico da mesma forma que os da rede corporativa? Eles devem incluir o ambiente doméstico em seus programas de gerenciamento de vulnerabilidades? Estas são questões de arquitetura importantes.

3 Simplificando a segurança da rede

O SASE promete mais do que apenas segurança; promete simplicidade. As redes atuais são muitas vezes sobrecarregadas por uma mistura de produtos de segurança de diferentes fornecedores. Estes portfólios crescem organicamente ou por meio de aquisições, criando conjuntos de soluções incompatíveis e complexos que são difíceis e demorados de gerenciar. Eles afetam o desempenho da rede e dificultam a segurança.

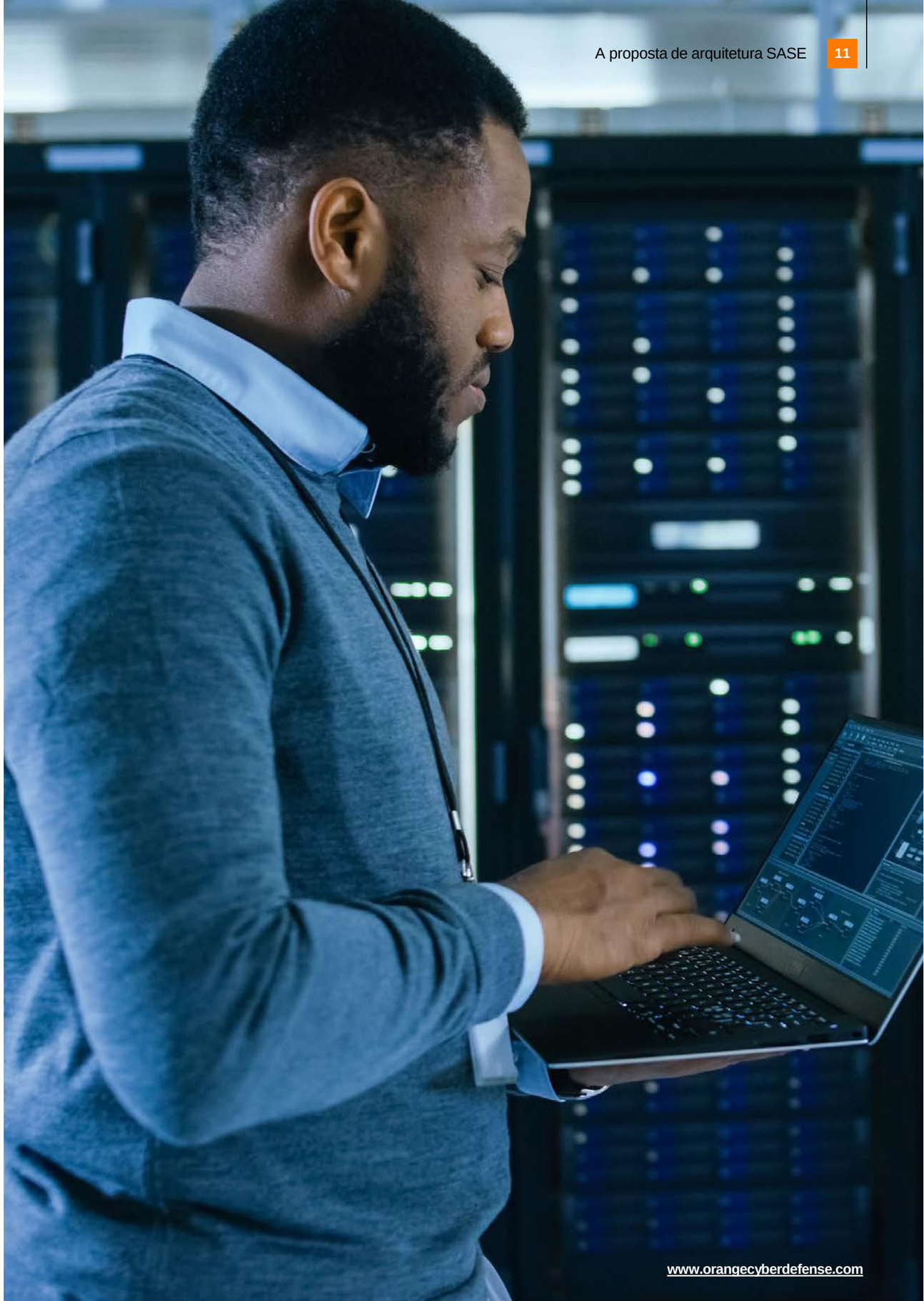
O modelo SASE consolida esses ambientes fragmentados de segurança cibernética em uma plataforma mais simples e unificada, envolvendo um menor conjunto de fornecedores. Isso garante uma segurança ideal em todas as partes da rede e promove a interoperabilidade, capturando as ameaças antes que elas escapem pelas fendas. Também reduz o impacto das ferramentas de segurança sobre o desempenho e o custo.

4 Para além do SD-WAN



Após definir o que é SASE, é importante articular o que o SASE não é. O SASE não é apenas SD-WAN.
SD-WAN ainda é um termo jovem o suficiente para que as implementações do fornecedor variem muito, tornando difícil fornecer um componente de segurança cibernética confiável e consistente. Muitos deles prestam serviços de segurança através dos equipamentos das instalações do cliente que pode ser custoso de implementar.
Tampouco é apenas segurança baseada na nuvem. Serviços de segurança cibernética baseados na nuvem que não se integram perfeitamente com funcionalidades de rede definidas por software perdem as vantagens da proteção de confiança zero, desempenho e política de segurança uniforme do SASE.
A combinação das ofertas de rede e segurança do SASE é uma abordagem mais simples, mais barata e mais flexível para a segurança cibernética do que pensar em SD-WAN e segurança separadamente. Colocar os serviços de segurança cibernética na rede definida por software como serviços nativos das nuvens em POPs de ponta facilita a implementação e o gerenciamento.
O SASE também é mais do que apenas estas tecnologias combinadas. Embora o SASE priorize a automação como um meio de escalar o acesso seguro, ele funciona melhor quando discutido como parte de uma proposta baseada em serviços. As empresas devem alimentar sua rede de segurança com dados de qualidade que evidenciem as ameaças emergentes de agentes maliciosos. Elas também devem monitorar constantemente as operações da rede para observar sinais de comprometimento e responder de acordo.

> “ A combinação das ofertas de rede e segurança do SASE é uma abordagem mais simples, mais barata e mais flexível para a segurança cibernética do que pensar em SD-WAN e segurança separadamente.



A importância da identidade

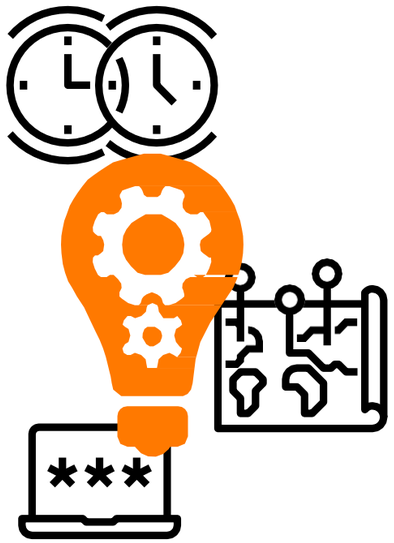
O SASE combina rede e segurança, fornecendo ambos como um serviço com base na nuvem, mas nosso foco é a segurança da rede.

A identidade sustenta esses serviços de segurança de rede em um ambiente SASE. Esta é a chave que torna possível a aplicação de políticas automatizadas.

O SASE toma decisões baseadas no contexto ao aplicar as políticas que regem a segurança e os privilégios de acesso. A principal parte dos dados que contribuem para esse contexto é a identidade do usuário, dispositivo ou serviço que acessa o recurso. Outros parâmetros, incluindo localização, tempo de acesso, nível de confiança e os dados solicitados, também afetam esse contexto.

Como todos estes parâmetros podem mudar entre as sessões, as políticas de segurança cibernética se adaptam a cada sessão em um ambiente SASE.

“ A identidade sustenta esses serviços de segurança de rede em um ambiente SASE. Esta é a chave que torna possível a aplicação de políticas automatizadas.



Orientação

Discutimos o ambiente SASE ideal, mas devemos ser realistas; daqui até lá envolverá muito trabalho pesado. Os caminhos para uma solução SASE também são variados, e os detalhes de implementação dependerão do contexto e dos objetivos da empresa.

O Gartner descreve inúmeros riscos em seu relatório, e muitos deles decorrem da mesma preocupação central: a falta de capacidade do fornecedor.

Aconselhamos que você discuta seus planos de arquitetura SASE a longo prazo com MSPs focados em segurança. Pense além de suas escolhas tecnológicas, considerando também as políticas e perfis de segurança que essas tecnologias relacionadas com o SASE suportarão. A inspeção e aplicação dinâmica do tráfego com base no contexto - um dos princípios fundamentais de uma solução de acesso à rede de confiança zero - deve ser uma prioridade ao planejar uma arquitetura SASE.

Uma iniciativa SASE será um longo caminho. Ela redefine como a maioria das organizações aborda a segurança em um nível básico e toca cada parte de sua infraestrutura. Uma mistura de inércia organizacional, investimento irrecuperável e dívida técnica tornam este projeto uma proposta de longo prazo.

Fique ágil

Com isto em mente, a mudança para o SASE terá uma série de etapas graduais. Considere os principais requisitos deste modelo ao renovar projetos existentes ou implementar novos projetos, especialmente em torno de serviços de segurança como SWG, CASB e VPNs.

Procure oportunidades de consolidação a curto prazo ao avaliar estas renovações, substituições e novos desenvolvimentos. Agora é o momento de combinar os serviços existentes, simplificando e desduplicando funcionalidades. Explore as decisões de compra de um ponto de vista estratégico, entendendo como elas se encaixarão na arquitetura SASE mais ampla, em vez de se concentrar apenas nas características isoladas do produto.

Qualquer compra ou remodelação é uma oportunidade de transição de serviços legados para uma arquitetura definida por software, gerenciável a partir de um único console. Foco na eliminação de silos de segurança e na integração de produtos para apoiar políticas unificadas através de inspeção de passagem única.

Estas decisões de arquitetura informarão a capacidade de escala da infraestrutura de segurança. Elas aumentarão sua capacidade de adaptação às ameaças e pressões em constante mudança.

Adote uma abordagem de mini-plataforma

Embora um modelo SASE enfatize a consolidação, acreditamos ser irrealista confiar em um único fornecedor para fornecer todas essas peças móveis. Mesmo que as empresas sejam capazes de reduzir o número de fornecedores de segurança cibernética com os quais trabalham, elas não serão capazes de adquirir uma solução de um único fornecedor que cubra todas as suas bases.

Por exemplo, um requisito para uma solução SASE é a inspeção do tráfego criptografado em escala. Isto é especialmente importante em um ambiente que aplica múltiplas proteções cibernéticas de segurança a esse tráfego. Nem todos os fornecedores apoiarão esta inspeção de tráfego criptografado para processamento de passagem única e multisserviços no nível esperado.

> “Você deve insistir em contratos de curto prazo com licenças flexíveis ao negociar com os fornecedores para manter suas opções em aberto durante um período de rápida evolução e mudança.

Outras exigências aos fornecedores incluem a conscientização do contexto dos dados, que vai além da inspeção de tráfego criptografado para ver como os dados estão sendo usados em um ambiente de nuvem. Isso exige a inspeção de ambientes de provedores de serviços na nuvem em comparação com interfaces de programação de aplicações. Nem todos os fornecedores conseguirão isso.

A capacidade dos vendedores se desempenharem bem na nuvem também é uma preocupação central para o Gartner. Preocupa que os fornecedores presos a equipamentos de hardware possam ter dificuldade de transição para a prestação de serviços nativos da nuvem, crucial em um ambiente SASE.

Em vez de depender de um único fornecedor, adote uma abordagem de mini-plataforma, reduzindo seus portfolios de fornecedores. Encontre conjuntos de soluções que dependam de três a cinco fornecedores, e substitua-os por soluções de um único fornecedor. Isto equilibra as melhores capacidades da categoria com eficiências operacionais. Você deve insistir em contratos de curto prazo com licenças flexíveis ao negociar com os fornecedores para manter suas opções em aberto durante um período de rápida evolução e mudança.

Mesmo que muitas destas decisões de compra não se concretizem por algum tempo, você pode começar agora a desafiar os fornecedores com estas exigências emergentes e a tornar seus critérios de compra conhecidos. Discuta seu roteiro tecnológico com fornecedores de rede e serviços de segurança para identificar soluções SD-WAN, SWG, CASB e ZTNA de curto e longo prazo. O foco na estratégia de integração deve ser uma parte fundamental destas conversas porque os fornecedores frequentemente construirão suas ofertas SASE via aquisição.

Conduza a segurança a partir do topo

O SASE é uma iniciativa cultural, não apenas técnica. Seu sucesso depende da cooperação de várias equipes em toda a organização, muitas das quais podem estar enraizadas e ambivalentes em relação à mudança.

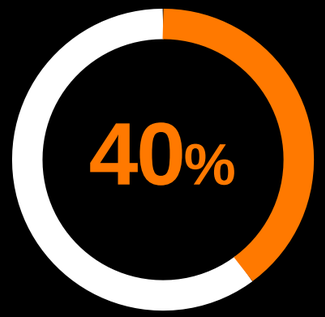
As empresas interessadas no SASE devem estar dispostas a conduzir a segurança a partir do topo, garantindo a adesão da gerência sênior. Nomear executivos C-suite com o poder de impulsionar mudanças e superar resistências políticas em nível de equipe. Esteja preparado para o longo prazo, pois esta transição cultural levará tempo, persistência e paciência.

Envolva o CISO desde o início

O SASE impulsiona a segurança na infraestrutura da rede, tornando-a um componente fundamental de todo fluxo de trabalho corporativo. Agora, mais do que nunca, a equipe de segurança precisa de um lugar à mesa.

O CISO (Executivo-Chefe de Segurança da Informação) deve estar envolvido em todas as discussões que envolvem a aquisição ou transformação de uma nova rede ou solução de segurança de rede, internamente e com fornecedores e arquitetos líderes. Esta equipe deve ajudar a avaliar as ofertas e guias de cada fornecedor.

Uma estratégia de adoção do SASE



O Gartner prevê que 40% das empresas terão uma estratégia SASE até 2024, mas há uma longa jornada entre a estratégia e a realidade. As empresas devem começar a se preparar agora para uma mudança arquitetônica e cultural tão ampla como o SASE.

De fato, muitos têm pouca escolha porque a pandemia forçou sua decisão; eles já precisam adotar alguns elementos do SASE, como o acesso à rede de confiança zero em resposta à necessidade de trabalho remoto. Aqui estão alguns itens a serem feitos para seu roteiro de adoção.

1 Faça o caso de negócios (business case)

Comece por defender o SASE entre os principais responsáveis pela tomada de decisões. Isto envolve tanto um caso estratégico de longo prazo quanto propostas menores e mais imediatas como parte de uma implantação gradual.

2 Crie sinergia entre as equipes de segurança e de rede

As equipes de segurança e rede muitas vezes vivem em silos, mas ao projetar e implantar o modelo SASE, elas não conseguem falar com frequência suficiente. Comece a construir sinergia entre estes grupos o mais cedo possível para facilitar ainda mais o trabalho de integração ao longo do caminho.

3 Avalie o impacto operacional e organizacional sobre as redes e a segurança

Ao elaborar uma proposta de arquitetura de longo prazo para o SASE, as equipes de projeto devem considerar o impacto operacional em seus sistemas.

4 Inicie a transformação SD-WAN

O SASE precisa de uma plataforma de rede definida por software para a implantação de serviços baseados em edge cloud. Isso envolve a mudança para uma arquitetura SD-WAN, incluindo a transição de MPLS para conexões de Internet. É crucial enfrentar esta etapa tendo em mente serviços de segurança de rede definidos por software, incluindo uma solução de acesso remoto no sistema SD-WAN em um estágio inicial para garantir uma segurança consistente para os trabalhadores remotos.

5 Migre os serviços de segurança cibernética do centro de dados existente para a nuvem

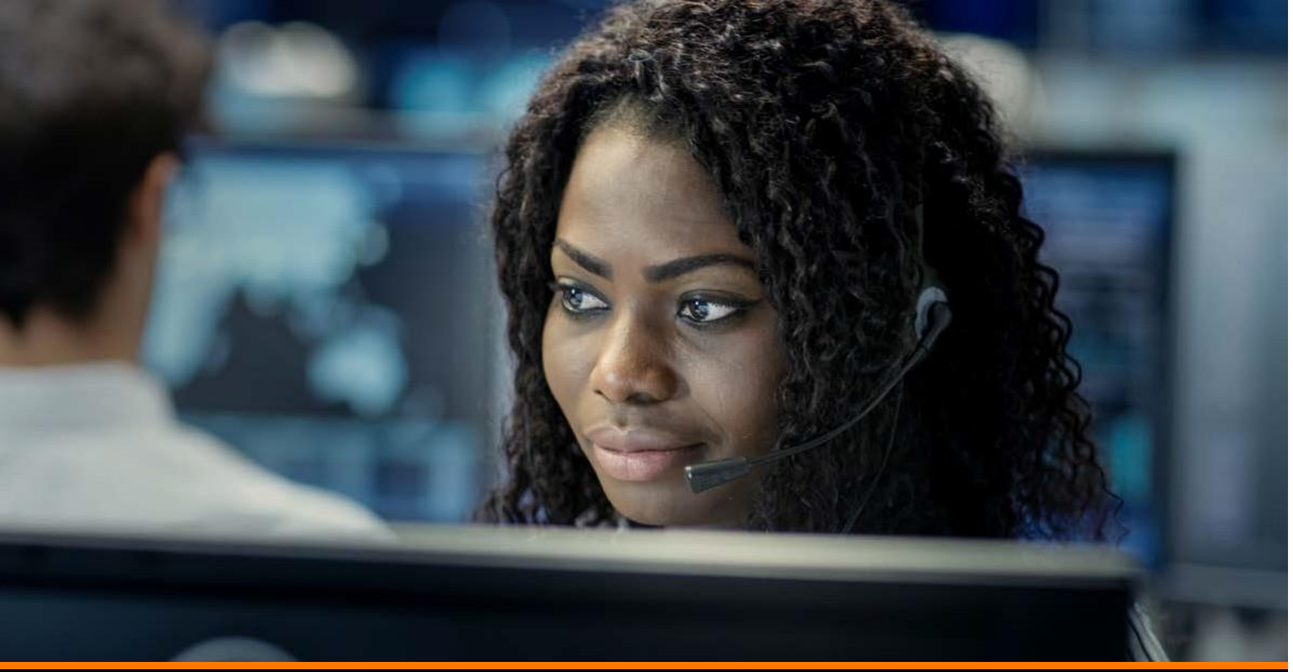
Com uma solução SD-WAN em vigor, é hora de planejar a mudança do sistema antigo de serviços de segurança local para POPs habilitados para nuvens, operando na rede definida por software. Isso significa fazer a transição para um provedor de segurança na nuvem.

6 Mudar a postura e o design de segurança para o acesso à rede de confiança zero

Você deve fazer a migração para serviços de segurança com base na nuvem com o acesso à rede de confiança zero em mente. Isso inclui o planejamento de acesso com base na identidade para todas as aplicações. Construa componentes incluindo gerenciamento de identidade e acesso e estruturas de gerenciamento do ciclo de vida da identidade que apoiarão a migração para o acesso com base na identidade. Agora também é um bom ponto para considerar tecnologias complementares como autenticação multi-fator e controle de acesso à rede com base em dispositivos para proteger dispositivos móveis gerenciados que acessam aplicações corporativas.

7 Desenvolva uma estrutura de automação

Com um sistema de segurança de rede definido por software, você estará bem posicionado para impulsionar novas eficiências em sua infraestrutura de segurança usando automação. Invista na criação e refinamento de um plano de controle de rede e segurança definido por software que formará a base de uma operação de segurança robusta e adaptável.



Sobre a Orange Cyberdefense

A Orange Cyberdefense é a unidade de negócios especializada em segurança cibernética do Grupo Orange. Como fornecedor "go-to security" da Europa, nos esforçamos para construir uma sociedade digital mais segura.

Somos um provedor de segurança orientado por inteligência e pesquisa de ameaças que oferece acesso inigualável a ameaças atuais e emergentes.

A Orange Cyberdefense mantém um histórico de mais de 25 anos em segurança da informação, mais de 250 pesquisadores e analistas 18 SOCs, 11 CyberSOCs e 4 CERTs distribuídos em todo o mundo e suporte de vendas e serviços em 160 países. Temos orgulho de dizer que podemos oferecer proteção global com experiência local e apoiar nossos clientes durante todo o ciclo de vida da ameaça.

Twitter: @OrangeCyberDef

Fuentes:
1. IDC - https://www.idc.com/getdoc.jsp?containerId=prUS46934120 European Commission – https://ec.europa.eu/jrc/sites/jrcsh/files/jrc120945_policy_brief_-_covid_and_telework_final.pdf
2. IDC Webinar - Envisioning a Resilient Cloud Based Digital Infrastructure webinar April 2020
3. US Cybersecurity and Infrastructure Security Agencies - https://us-cert.cisa.gov/ncas/alerts/aa20-099a
4. IDC - https://www.idc.com/getdoc.jsp?containerId=prAP46737220#:~:text=IDC%20estimates%20data%20generated%20from,significant%20portion%20of%20this%20data

Orange
Cyberdefense

orange™