Trazido para você por:

netskope

Desenvolvendo uma Arquitetura SASE

para leigos

Domine a segurança na nuvem

Aborde as principais mudanças em aplicações, dados, segurança e redes

Melhore e mantenha a experiência do usuário

Edição especial da Netskope

Jason Clark
Lamont Orange
Steve Riley

Sobre a Netskope

A Netskope, líder em SASE, conecta os usuários com segurança e rapidez diretamente à Internet, a qualquer aplicação e a sua infraestrutura a partir de qualquer dispositivo, dentro ou fora da rede. Com CASE, proxy e ZTNA construídos nativamente em uma única plataforma, a Netskope é rápida em qualquer lugar, centrada em dados e cloud smart, ao mesmo tempo que permite uma boa cidadania digital e fornece um custo total de propriedade menor. Acesse www.netskope.com para conhecer mais.

Gostaríamos de agradecer a várias pessoas que tornaram possível a publicação deste livro:

Da Netskope: Amanda Anderson, Mike Anderson, Chad Berndtson, James Christiansen, Tom Clare, Mark Day, David Fairman, Maxwell Havey, Scott Hogrefe, Kathy Jacobsen, Greg Mayfield, Mariesa Milan, Sasi Murthy, Krishna Narayanaswamy, Lauren Polito, Kate Reid, Zoe Revis, Brian Tokuyoshi

Da Evolved Media: Karen Queen, Evan Sirof, Lauren Wagner, Dan Woods

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

Desenvolvendo uma arquitetura SASE

Edição Especial da Netskope

Jason Clark, Lamont Orange, Steve Riley

para leigos®

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

Desenvolvendo uma arquitetura SASE para leigos®, Edição Especial da Netskope

Publicado por
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

Copyright © 2022 por John Wiley & Sons, Inc., Hoboken, Nova Jersey

Nenhuma parte desta publicação poderá ser reproduzida, armazenada em um sistema de recuperação ou transmitida de qualquer forma ou por qualquer meio, eletrônico, mecânico, fotocópia, gravação, digitalização ou de outra forma, exceto conforme permitido nas Seções 107 ou 108 da Lei de direitos autorais dos Estados Unidos de 1976, sem a prévia autorização por escrito da Editora. Os pedidos para permissão da Editora devem ser enviados para Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008 ou on-line pelo site http://www.wiley.com/go/permissions.

Marcas registradas: Wiley, For Dummies, o logotipo Dummies Man, The Dummies Way, Dummies.com, Making Everything Easier e imagens comerciais relacionadas são marcas comerciais ou marcas registradas da John Wiley & Sons, Inc. e/ou de suas afiliadas nos Estados Unidos e outros países, e não poderão ser utilizadas sem permissão por escrito. Todas as marcas registradas pertencem a seus respectivos proprietários. A John Wiley & Sons, Inc., não está associada a nenhum produto ou fornecedor mencionado neste livro.

LIMITAÇÃO DE RESPONSABILIDADE / RENÚNCIA DE GARANTIA: A EDITORA E O AUTOR NÃO FAZEM DECLARAÇÕES OU GARANTIAS RELATIVAMENTE À PRECISÃO OU À INTEGRIDADE DO CONTEÚDO DESTA OBRA E, ESPECIFICAMENTE, RENUNCIAM A TODAS AS GARANTIAS, INCLUSIVE, ENTRE OUTRAS, GARANTIAS DE APTIDÃO PARA UM DETERMINADO PROPÓSITO. NENHUMA GARANTIA PODERÁ SER CRIADA OU ESTENDIDA POR VENDAS OU MATERIAIS PROMOCIONAIS. AS ORIENTAÇÕES E AS ESTRATÉGIAS CONTIDAS NO PRESENTE DOCUMENTO PODERÃO NÃO SER ADEQUADAS PARA TODAS AS SITUAÇÕES. ESTA OBRA É VENDIDA COM O ENTENDIMENTO DE QUE A EDITORA NÃO PRESTA SERVIÇOS JURÍDICOS, CONTÁBEIS OU OUTROS SERVIÇOS PROFISSIONAIS. SE FOR PRECISO ASSISTÊNCIA PROFISSIONAL, DEVEM SER USADOS OS SERVIÇOS DE UM PROFISSIONAL COMPETENTE. NEM A EDITORA NEM O AUTOR SERÃO RESPONSÁVEIS POR DANOS PROVENIENTES DESTA OBRA. O FATO DE QUE UMA ORGANIZAÇÃO OU UM SITE É MENCIONADO NESTA OBRA COMO UMA CITAÇÃO E/OU UMA FONTE POTENCIAL DE INFORMAÇÕES ADICIONAIS NÃO SIGNIFICA QUE O AUTOR OU A EDITORA APROVE AS INFORMAÇÕES QUE A ORGANIZAÇÃO OU O SITE OFEREÇA OU RECOMENDAÇÕES QUE FAÇA. ALÉM DISSO, OS LEITORES DEVEM ESTAR CIENTES DE QUE OS SITES DA INTERNET LISTADOS NESTA OBRA PODEM SER ALTERADOS OU RETIRADOS NO PERÍODO EM QUE O LIVRO FOI ESCRITO E QUANDO FOR LIDO.

Para obter informações gerais sobre nossos outros produtos e serviços, ou sobre como criar um livro personalizado *For Dummies* para sua empresa ou organização, entre em contato com nosso Departamento de Desenvolvimento de Negócios nos EUA pelo telefone 877-409-4177, pelo e-mail info@dummies.biz ou visite www.wiley.com/go/custompub. Para obter informações sobre o licenciamento da marca *For Dummies* para produtos ou serviços, entre em contato pelo e-mail BrandedRights&Licenses@Wiley.com.

ISBN 978-1-119-85518-7 (pbk); ISBN 978-1-119-85519-4 (ebk)

Fabricado nos Estados Unidos da América

10 9 8 7 6 5 4 3 2 1

Agradecimentos da Editora

Algumas das pessoas que ajudaram a colocar este livro no mercado são:

Editora do projeto: Elizabeth Kuball

Responsável por aquisições: Ashley Coffey

Gerente editorial: Rev Mengle

Representante de desenvolvimento de negócios: William Hull

Responsável pela produção: Vivek Lakshmikanth

Ajuda Especial: Nicole Sholly

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

Introdução

Seus funcionários, parceiros e clientes usam cada vez mais a nuvem em vez de redes privadas e data centers. A segurança não pode inibir a maneira como eles trabalham. Enquanto isso, você e outros líderes de negócios estão lutando para realinhar a segurança em um ambiente que, se usar ferramentas de segurança tradicionais, estará fora de seu controle. Esse equilíbrio entre segurança e experiência do usuário é difícil de alcançar em tempos "normais", mas nenhum catalisador desafiou as organizações como a pandemia da COVID-19, que levou milhões de trabalhadores para casa.

A complexidade do cenário de segurança desafiou até mesmo as melhores equipes de segurança e aumentou a chance de configurações incorretas e violações. Produtos, serviços e mensagens conflitantes do setor tornam um desafio aos decisores de segurança aproveitar as oportunidades enquanto refatoram a segurança para atender às suas necessidades.

Uma arquitetura emergente de rede e segurança chamada de secure access service edge (SASE; pronuncia-se "sássi") aponta o caminho a seguir. Next generation secure web gateways (NG SWGs), cloud access security brokers (CASBs) e princípios de Confiança Zero (Zero Trust), representam elementos essenciais para a arquitetura SASE que combina serviços de rede e serviços de segurança de rede em um sistema unificado para proteger os interesses comerciais e a funcionalidade da nuvem. Mas como arquitetar tudo da maneira certa e na sequência certa? É aí que entra este livro.

Sobre Este Livro

Este livro pode ajudá-lo a desenvolver um roteiro para a implementação de projetos de rede e segurança que fornecerão resultados positivos e incrementais no curto prazo, enquanto pavimentam o caminho para um futuro resiliente e seguro que prioriza a nuvem. Ele esclarece as bobagensque você ouve de supostos fornecedores de SASE, fornecendo uma compreensão prática do que SASE é – e o que não é – e permitindo preparar seus investimentos, em segurança e redes, para o futuro e garantir que a adaptação às mudanças inevitáveis seja a mais fácil e mais econômica possível.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

Suposições Tolas

Você já está habituado à Internet. Você sabe que ela é o lar de uma grande variedade de ferramentas digitais baseadas em nuvem, que as pessoas usam para necessidades profissionais e pessoais – ferramentas que estão em uso sem o envolvimento, e muito menos a aprovação, das equipes de segurança e TI. Você também está ciente de que a nuvem pode ser um lugar perigoso onde as credenciais e os dados de indivíduos e empresas têm sofrido ataques. Por último, você tem interesse em resolver esse desafio para sua empresa, funcionários, acionistas, clientes e parceiros de negócios.

Ícones Usados neste Livro

Usamos ícones na margem para chamar a atenção para informações importantes. Aqui está o que você pode esperar:

DICA

Qualquer coisa marcada com o ícone Dica é um atalho para facilitar uma tarefa específica.

LEMBRETE

O ícone Lembrete sinaliza fatos que são especialmente importantes para saber.

MATERIAL TÉCNICO

Quando oferecemos informações altamente técnicas que você pode ignorar com segurança, usamos o ícone de Material Técnico.

ATENÇÃO

Preste atenção a qualquer coisa marcada com o ícone Atenção para evitar algumas dores de cabeça.

Além do Livro

Embora este livro esteja repleto de informações, se ao final você pensar: "Onde posso aprender mais?", vá para `www.netskope.com/pt/`.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

NESTE CAPÍTULO

- **Reconhecendo como a natureza da segurança mudou na era da nuvem**
- **Identificando como as práticas de segurança pré-nuvem criam novos problemas**
- **Conhecendo SASE e como ele viabiliza a nuvem para os negócios**
- **Gerando valor duradouro para o negócio com uma arquitetura SASE que funciona**
- **Dissociando o valor de SASE do ruído publicitário**

Capítulo 1
Entendendo a Visão de SASE para Proteger Empresas Focadas em Nuvem

O termo *nuvem* é lançado com tanta frequência que pode ser difícil saber o que significa. Em termos de aplicações – e em termos bastante simplificados – o termo *nuvem* pode se referir a:

- **Nuvem privada:** aplicações em seu data center.
- **Nuvem pública:** significa muitas coisas, incluindo infraestrutura como serviço (IaaS) e plataforma como serviço (PaaS), mas para simplificar, pense na nuvem pública como aplicações disponíveis na Internet pública.
- **Nuvem privada virtual:** aplicações privadas acessíveis a partir da nuvem pública.
- **Software como serviço (SaaS):** aplicações hospedadas por um fornecedor terceirizado e acessadas pela Internet.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

Esta utilização casual da palavra *nuvem* pode dificultar a avaliação das opções e sua relação com suas necessidades específicas. Comece entendendo o que você precisa que a segurança faça. Essas informações ajudarão a esclarecer as questões, porque você precisa desses recursos em todas as interações em nuvem.

Neste capítulo, você descobrirá como a nuvem mudou a segurança, por que a segurança pré-nuvem não funciona mais na era da nuvem, por que as abordagens de rede tradicionais como *hairpinning* não funcionam, como o secure access service edge (SASE) pode permitir aos seus funcionários trabalhar de forma segura e produtiva na nuvem e os fatores que definem o melhor SASE da categoria.

CHEGA DE NICHO

Vulnerabilidades centradas na nuvem não podem mais ser consideradas como "nicho". Desde 2021:

- O número de aplicações em nuvem em uso por organização aumentou 20% em relação ao ano anterior. Organizações com 500 a 2.000 funcionários agora usam, em média, 664 aplicações distintas em nuvem por mês, de acordo com um relatório de fevereiro de 2021 da Netskope.
- 61 por cento dos downloads de malware poderiam ser rastreados até o armazenamento em nuvem e aplicações colaborativas em dezembro de 2020, contra 48 por cento em janeiro de 2020, de acordo com o relatório da Netskope.
- 55 por cento das sessões estão relacionadas a aplicações e serviços em nuvem no tráfego da Web, de acordo com o relatório da Netskope.
- 83 por cento dos usuários acessam aplicações pessoais em dispositivos gerenciados por empresas, de acordo com o relatório da Netskope. Este é o problema de segurança urgente que você deve abordar: como permitir que sua organização aproveite ao máximo tudo que a nuvem pode oferecer em termos de flexibilidade, gerenciamento de custos e novas abordagens para oportunidades de negócios, ao mesmo tempo que mantém seus usuários de negócios, clientes, dados e outros recursos preciosos, seguros em todos os momentos.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

Como a Nuvem Mudou a Segurança e as Redes

Era uma vez data centers corporativos que eram as poderosas fortalezas do mundo dos negócios. As empresas ergueram essas cidadelas digitais e, em seguida, criaram e implantaram aplicações de negócios dentro de suas muralhas. Dentro da fortaleza, as empresas estabeleceram redes privadas que conectavam pessoas aos dados, incluindo funcionários na matriz, funcionários em escritórios remotos e funcionários viajando pelo mundo.

Como todos os grandes castelos, havia um perímetro óbvio: uma muralha com um portão protegido. O acesso para entrar e sair dos confins da Internet além do portão era estritamente regulamentado. Os guardiões podiam ficar de olho no tráfego ao longo de suas poucas estradas protegidas, permitindo a entrada dos justos, evitando qualquer coisa suspeita e entrando em ação ao primeiro sinal de problema. Cada intercâmbio com o mundo exterior era forçado a voltar aos confins da rede privada.

Primeiro um gotejamento, depois uma torrente de usuários corporativos gravitou para aplicações em nuvem. As aplicações em nuvem – para redes sociais e comunicação, para colaboração e para analisar os detalhes de vendas, finanças, marketing e relacionamento com o clientes – eram simplesmente melhores do que qualquer outra coisa oferecida internamente. Em seguida, as empresas e até mesmo as agências governamentais de evolução mais lenta entraram a bordo. As organizações de hoje favorecem as aplicações SaaS e adotaram políticas abrangentes focadas em nuvem que exigem a solução de desafios de negócios com soluções em nuvem e a transferência de sistemas corporativos essenciais para a nuvem.

As coisas mudaram quando poderosas novas aplicações foram disponibilizadas na nuvem. Pessoas, dispositivos e aplicações são móveis dentro e fora de sua rede. Os produtos SaaS fornecem recursos fantásticos para as empresas, mais rápidos e melhores do que as abordagens anteriores que exigiam longos tempos de desenvolvimento e aquisição de hardware e de software.

No final da última década, o crescimento dos gastos com atividades em nuvem aumentou significativamente, ultrapassando em muito o ritmo de todas as outras partes dos orçamentos de TI, de acordo com o Synergy Research Group. Em 2024, mais de 45 por cento dos gastos de TI em infraestrutura de sistemas, software de infraestrutura, aplicações e terceirização de processos de negócios passarão das soluções tradicionais

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

para a nuvem, tornando a computação em nuvem uma das forças mais continuamente revolucionárias nos mercados de TI desde o início da era digital, de acordo com o Gartner.

No entanto, muitas dessas ferramentas em nuvem permanecem fora da visibilidade e do controle dos departamentos de TI. Do ponto de vista da segurança, isso é preocupante. Mas a segurança não significa apenas proteger aplicações em nuvem.

Segurança também significa fornecer toda a proteção necessária quando toda a sua força de trabalho estiver trabalhando remotamente. Onde quer que estejam, seus usuários precisam ser protegidos contra ataques e manter dados e aplicações seguros. E do ponto de vista da rede, a experiência precisa ser não apenas segura, mas também funcional. A segurança não pode ser um gargalo para a produtividade que os usuários percebem quando podem usar a nuvem para fazer mais coisas com mais rapidez, onde quer que estejam.

Depois existem as informações. Os dados (tudo, desde propriedade intelectual e números de vendas até números de cartão de crédito de clientes) são um tesouro valioso que sua empresa possui – talvez mais valioso do que os produtos que você vende. O fato de a segurança de TI ser o assunto das manchetes de primeira página não é surpreendente; e quando é, as notícias raramente são boas. Com dados, aplicações e pessoas operando principalmente na nuvem, antigas técnicas de segurança desenvolvidas principalmente para data centers locais e outras infraestruturas tradicionais têm dificuldade em acompanhar. O mundo viu uma onda crescente de ataques de diversos hackers usando técnicas sofisticadas para causar estragos e explorar vulnerabilidades em aplicações em nuvem e na forma como elas são acessadas.

A transição para a nuvem não tem sido fácil nem descomplicada. As velhas estradas que atravessam a rede do data center estão repletas de obstáculos, incômodos e ineficiências que reduzem a produtividade, frustram os usuários e comprometem a segurança. As aplicações baseadas no data center são insignificantes em comparação com as aplicações SaaS em termos de produtividade, experiência do usuário e praticidade. As melhoriasde extrema necessidade trazidas pelo SaaS capacitaram os vendedores a vender mais, os times de marketing a amplificar suas mensagens, os departamentos de RH a encontrar os melhores candidatos e os desenvolvedores de produtos a trabalhar mais rápido. Desistir do SaaS significaria abrir mão de uma produtividade sem precedentes. Nenhuma empresa quer isso.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

O problema era que essas aplicações SaaS exigiam que os dados de dentro das muralhas fossem úteis e, mesmo assim, as aplicações estavam fora das muralhas, portanto não eram controlados ou protegidos por segurança. A segurança corporativa, sabendo que tinha muito pouco controle sobre as coisas "lá fora" na nuvem, tinha duas opções: dizer não ou fingir não notar. Isso hoje é descrito como *shadow IT*, onde usuários e até departamentos inteiros driblam a TI e a segurança para usar ferramentas SaaS como Salesforce e Google Docs, bem como grandes ferramentas de compartilhamento de arquivos como Dropbox que são práticas, mas não aprovadas para uso comercial. A shadow IT existe há muitos anos, mas seu uso (e risco) acelerou graças à adoção da nuvem. Os profissionais de segurança, com seus kits de ferramentas desenvolvidos para data centers corporativos e o estilo antigo de rastrear e controlar aplicações, encontram-se em um beco sem saída.

LEMBRETE

A velha segurança sempre exige concessões: as escolhas que elevam alguns padrões, como velocidade ou flexibilidade, vêm à custa de outras, designadas segurança. SASE, quando bem feito, é um facilitador. Ele permite que as pessoas mais próximas do problema inovem e resolvam problemas com tecnologia de maneira segura e controlada, ao mesmo tempo em que ajuda os líderes de TI a compreender melhor seus negócios.

Os Problemas da Segurança da Era Pré-Nuvem

Ferramentas, técnicas e tecnologias de segurança da era pré-nuvem ainda estão em uso em todos os lugares. Muito provavelmente, isso inclui a infraestrutura de TI da sua própria empresa. Isso cria uma situação em que muitas ferramentas de segurança estão em vigor, mas o resultado não tem nada a ver com segurança ou eficiência. Os problemas persistentes geralmente se enquadram em uma de duas categorias: a abordagem errada ou nenhuma abordagem estratégica.

A abordagem errada

Um dos benefícios observados de um data center corporativo e a eficácia de sua segurança era que ele mantinha os ativos digitais de uma empresa em um local único e seguro. Uma empresa podia então construir sua própria rede privada para conectar os funcionários da matriz, bem como os das filiais, e controlar seu acesso aos bits de que precisavam no data center.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

LEMBRETE

As empresas ainda precisam de data centers. Mas hoje em dia, o data center é apenas um dos muitos lugares para onde os usuários e os dados vão. Ele não está mais no centro de nada, seja para as necessidades de negócios ou como um único ponto de controle de segurança.

Os sistemas de segurança para data centers geralmente são appliances – caixas físicas conectadas ao data center para atender a funções específicas e restritas. Ao longo dos anos, as empresas podem ter adquirido sistemas de segurança de centenas de fornecedores; em 2021, a empresa média comprou e implantou uma grande quantidade de produtos de segurança. Na maioria dos casos, esses produtos não foram projetados para funcionar juntos. É quase impossível para a equipe de segurança integrar todos esses sistemas em uma solução de segurança adaptável e orquestrada que possa aplicar políticas que ofereçam suporte a aplicações em nuvem e trabalhadores remotos.

ATENÇÃO

Ter diversos sistemas geralmente resulta em caos nos consoles (e talvez em discussões sobre quem controla quais consoles). Sua equipe de segurança e rede pode enfrentar dezenas de tipos de gerenciamento diferentes, cada um com suas próprias prioridades e todos competindo por atenção. Pode ser impossível compreender o quadro geral ou uma única situação quando você está prestes a diagnosticar um problema. Processos de segurança como esses também são reativos, geralmente contando com logs para reproduzir e diagnosticar o que aconteceu. Pior, essa tigela de espaguete de sistemas dificulta estabelecer o tipo de ordem que tornaria tudo mais seguro. Você pode alcançar essa ordem e segurança apenas criando um sistema de regras detalhadas com as nuances para manter automaticamente a segurança em toda a variedade infinita de interações digitais.

LEMBRETE

O papel da segurança não é apenas dizer "não". Você quer dizer "sim" para coisas que permitem que sua empresa trabalhe com mais rapidez e eficácia, especialmente com uma força de trabalho distribuída. A segurança deve priorizar a proteção de usuários e dados, mas também deve se adaptar em tempo real para acompanhar os requisitos em constante mudança. Isso significa fornecer aos usuários uma experiência de trabalho estável e produtiva onde quer que estejam, permitindo que acessem os dados de que precisam através de ferramentas que lhes permitam ser mais produtivos e bem-sucedidos.

Nenhuma abordagem

Seus usuários estão em qualquer lugar e a rede atual precisa ser projetada com isso em mente. Tentar forçar repetidamente todo o tráfego de um usuário através dos diversos serviços de segurança do data center restringe a produtividade. (Às vezes, os profissionais de segurança

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

e de rede chamam esta tática de *hairpinning*, o que significa forçar os usuários a desacelerar constantemente e mudar de direção, em vez de ir diretamente para onde precisam.) O *hairpinning* resulta em sistemas comerciais menos utilizáveis, desempenho drasticamente reduzido e usuários frustrados.

Qual é o tamanho do desafio de controlar este novo ambiente? Aqui está um exemplo: o Instituto Nacional de Padrões e Tecnologia (NIST, National Institute of Standards and Technology) é incumbido pelo Congresso dos Estados Unidos a fornecer orientação sobre segurança cibernética a organizações. O NIST publicou uma Estrutura de Segurança Cibernética que identificou 400 pontos de controle a serem considerados para proteger aplicações em sua organização. Este número provavelmente é baixo porque pressupõe que tudo – o usuário, os dados, o aplicação e a rede – reside no mesmo local. E este não é mais o caso.

A grande variedade de controles que você tem para pessoas e serviços em sua rede não está disponível para seus sistemas de segurança quando se trata de aplicações SaaS. Sua estratégia deve ser proteger um cenário muito mais amplo, em tempo real, usando apenas três pontos de controle:

- Os dados, de sua propriedade, que entram e saem de aplicações SaaS
- A identidade de cada usuário que está acessando essas aplicações
- Aprovação com base no fato de sua empresa realizar negócios com a entidade externa

LEMBRETE

A chave para uma segurança de nuvem bem-sucedida está em ajustar seu foco. Os sistemas de segurança anteriores eram amplamente baseados no controle de acesso. Eles eram as muralhas e os guadiões do castelo. Esta abordagem de castelo e portão não funciona mais. Para que a segurança na nuvem seja bem-sucedida, você deve se concentrar não no acesso, mas na atividade: quem está fazendo o quê, como as aplicações estão sendo usadas, quais dados estão indo para onde. Se você está cansado de pensar em castelos, considere uma metáfora do basquete: é hora de mudar sua segurança de uma zona de defesa baseada em perímetro para uma defesa homem a homem baseada em atividades.

MATERIAL TÉCNICO

Os sistemas de segurança mais antigos geralmente sabem para onde o usuário está indo na Internet. Mas a aplicação SaaS que eles estão usando pode depender de dezenas, centenas ou mesmo milhares de recursos adicionais para preencher a página da Web que o usuário vê. Para proteger a nuvem, você precisa saber esses detalhes. Suas ferramentas legadas não fazem coisas como decodificar a segurança de

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

camada de transporte (TLS), o que permitiria que elas vissem o que está acontecendo dentro do tráfego de comunicação do usuário com aquela aplicação. Estas ferramentas também não conseguem detectar certas conexões de interface de programação de aplicação (API) que a aplicação SaaS usa para trocar informações com outros recursos desconhecidos para construir um ambiente rico para o usuário. Sem este tipo de detalhe, você nunca pode ter certeza de que seus dados estão seguros ou que o que seu usuário está vendo foi proveniente de fontes legítimas.

Definindo SASE

Em um nível, SASE significa mover os controles de perímetro de segurança de rede para a nuvem, e ao mesmo tempo tornar esses controles mais rápidos, mais sensíveis à aplicação e ao usuário e centrados nos dados.

Em outro nível, SASE significa uma nova estratégia arquitetônica para segurança e rede que sua organização buscará alcançar. Ele aborda o fato de que um mundo centrado em nuvem precisa de um modelo atualizado para segurança e rede – e aborda as formas fundamentais nas quais a segurança, as redes, as aplicações e a proteção de dados foram transformados.

Funcionalmente, SASE compreende diversos serviços integrados e interligados de segurança e de rede desenvolvidos e fornecidos não apenas para conceder aos usuários acesso à nuvem, mas também para monitorar continuamente suas atividades, seus dispositivos e aplicações que usam para que os dados possam estar protegidos a todo momento, em cada ponto em que forem acessados, tudo sem sacrificar a experiência do usuário. A boa notícia é que a base de sua arquitetura de segurança SASE pode ser implantada hoje, e em etapas incrementais programadas (consulte o capítulo 5).

ATENÇÃO

Uma das características definidoras do SASE é que todos os aspectos desta arquitetura de segurança são desenvolvidos especificamente para uso na nuvem. Ele não reaproveita dispositivos ou códigos destinados a data centers. E você já sabe o motivo: os serviços de segurança para os data centers buscam principalmente controlar o acesso. Eles não falam a língua nativa da nuvem, que é rica em nuances e informações que descrevem as conexões entre os pontos e descrevem os dados contidos no fluxo de tráfego entre os pontos. Lembre-se disso ao avaliar as opções de segurança e de rede.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

O contexto é crucial e também é um guia informativo sobre o quão profunda e rica esta nova arquitetura de segurança pretende ser. Os fatores contextuais SASE são:

- A identidade do usuário
- O dispositivo que está sendo usado para solicitar acesso
- O local de onde o acesso está sendo tentado
- A identidade das aplicações acessadas na nuvem
- Os dados solicitados – o que são e onde estão armazenados
- Os padrões de comportamento do usuário
- A interação com a aplicação – o que o usuário está tentando fazer especificamente

Em seguida, ao reavaliar continuamente este fluxo dinâmico de informações, o sistema de segurança SASE aplica a segurança com base em políticas que determinam:

- O nível de serviço e o tipo de serviços de rede a serem aplicados
- O uso de tipos apropriados de criptografia de dados
- O nível de proteção de dados a ser aplicado para evitar o uso indevido de dados
- O nível de autenticação a ser aplicado
- Se a aplicação requer o uso de serviços de segurança específicos e especializados, como um agente de segurança de acesso à nuvem (CASB) para intermediar a atividade

LEMBRETE

Sim, muita coisa acontece em uma arquitetura SASE. Mas quando o SASE é verdadeiramente funcional e implementado de forma adequada, ele simplifica e melhora drasticamente a qualidade da segurança e a conectividade de rede. Quando o SASE é feito da maneira certa, todas essas coisas acontecem em tempo real, incluindo o gerenciamento de risco contínuo. Ao mover os serviços de segurança de seu data center para a nuvem, mais perto de seus pontos de vulnerabilidade e de seus usuários, você ganha maior visibilidade e controle mais firme sobre o que está acontecendo e com quem, a todo momento. O SASE ajuda as equipes de rede e de segurança na transição para permitir as novas aplicações e a maneira de fazer negócios, ao mesmo tempo em que protege o acesso às aplicações on-premises mais antigas.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

Os Benefícios Comerciais da Arquitetura SASE

As razões para adotar um modelo SASE para segurança, se alinham estreitamente com o valor que os negócios têm reconhecido amplamente na adoção da nuvem. A nuvem possibilita que pessoas e empresas trabalhem de forma mais eficaz, colaborativa, rápida, flexível e econômica. O SASE torna este progresso seguro.

Permitindo o crescimento dos negócios, que por sua vez acolhem a transformação digital

A segurança precisa ser como os freios de um carro rápido. Ela está lá para permitir uma movimentação rápida (porque você sabe que pode parar se necessário), para que possa gerenciar os riscos mais rapidamente. Ela não existe para retardar os negócios e impedi-los de se moverem rapidamente. Ela não existe para impedir a velocidade.

Você não pode fazer a transformação digital de forma segura sem transformar seus controles de segurança. À medida que as empresas adotam novas tecnologias para acelerar o crescimento e estar mais perto do cliente, a organização de TI pode ajudar significativamente a empresa movendo os controles de segurança para acompanhar o usuário e os dados, eliminando muitos atritos no processo. Dê a seus usuários as aplicações e o acesso de que precisam com treinamento no momento certo sobre sua utilização com segurança.

Acompanhando as mudanças

A nuvem oferece serviços essenciais em todos os aspectos do seu negócio, e novos casos de uso surgem diariamente. Sua empresa certamente aprovou alguns serviços em nuvem para seus usuários. E se houver um serviço de nuvem não aprovado que faz as coisas melhor, mais rápido e mais barato para indivíduos ou organizações inteiras, há uma grande probabilidade de que alguém em sua organização também esteja usando. Esta pessoa driblou a segurança, pagou a assinatura, baixou a aplicação e a usa todos os dias.

Reduzindo os custos

LEMBRETE

Há um dito comum, e repetido com frequência, em relação à segurança que diz: "Se você acha que a segurança é cara, espere até ver uma violação de segurança." De acordo com uma pesquisa publicada pela IBM e pelo Ponemon, o custo total médio de uma violação de dados é de

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

3,86 milhões de dólares. A maioria das empresas percebe que precisa de segurança, mas raramente avalia o quanto precisa dela até que tenha um problema.

A segurança é frequentemente vista como um centro de custo que é menos visível quando está funcionando bem. A segurança é, na verdade, um facilitador de negócios, mas mesmo colocando esta função de lado, o orçamento de segurança, amplo ou limitado, precisa ser gasto sabiamente. Infelizmente, gastos criteriosos e eficientes com segurança são algo contra os quais muitas organizações ainda relutam.

O SASE introduz importantes vantagens de eficiência de custos. Com sua abordagem altamente integrada aos serviços de segurança, o SASE pode ajudar a reduzir as despesas de capital, consolidando os recursos de muitos appliances de segurança no data center. Com menos sistemas para monitorar e manter, o SASE também reduz as despesas operacionais. Há mais economia na consolidação de fornecedores, design de rede aprimorado e interação eficiente com provedores de nuvem.

O SASE também ajuda a superar a já mencionada deficiência global de profissionais qualificados em segurança cibernética. Ao automatizar grande parte da atividade de detecção e de resposta, você pode reatribuir atividades de maior valor a uma equipe qualificada, como o desenvolvimento de políticas de segurança que permitem novas atividades de negócios aceleradas ou a construção de modelos de inteligência artificial (IA) que expandem a automação e a flexibilidade da infraestrutura de segurança. A arquitetura SASE torna melhor e mais adaptável o uso de membros individuais da equipe do que qualquer outra estrutura de segurança corporativa.

Mantendo a simplicidade

O erro humano é um dos principais contribuintes para o aumento da frequência de incidentes de segurança. Em parte, isso é um reflexo da enorme complexidade que os analistas de segurança humana enfrentam, o resultado direto de sistemas legados de segurança e de rede sendo usados para tarefas para as quais nunca foram concebidos. Esses sistemas lutam diariamente com um monstro de Frankenstein moderno, trazido à vida na forma de dezenas de aplicações de monitoramento que não falam uma linguagem comum entre si ou com as pessoas que os administram. O SASE fornece um plano claro para que muitos serviços de segurança possam trabalhar juntos de maneira compreensível.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

Derrubando Mitos sobre SASE

ATENÇÃO

Este provavelmente não é o primeiro livro *For Dummies* que você leu sobre SASE e provavelmente não será o último, embora seja nosso trabalho tornar este o melhor! Brincadeiras à parte, como acontece com qualquer tecnologia ou tendência emergente, o SASE está propício à desinformação. Assim como introduzir um *i* antes do nome de um produto não confere automaticamente elegância de design e adicionar um *e* não se traduz em potência e eficiência, o nome SASE já está sendo cooptado, exagerado e mal interpretado. Aqui estão vários mitos comuns.

Mito: SASE pode ser suportado por tecnologias legadas

A infraestrutura de segurança de rede atual é o produto de anos (em alguns casos, décadas) de desenvolvimento e de esforços de vendas. Mas nenhuma quantidade de patches, ajustes e maximização de vendas pode transformar dispositivos preexistentes em soluções de segurança nativas da nuvem. A nuvem exige uma nova abordagem.

Mito: SASE pode ser construído usando um proxy comum como base

Anteriormente, os proxies (SWGs) eram dedicados a controlar o acesso e a se defender contra ameaças da Web. O SASE tem uma função muito mais ampla que também inclui aplicações, serviços em nuvem, proteção de dados e prevenção contra perda de dados. (O capítulo 2 analisa em detalhes como os next generation secure web gateways [NG SWG] atendem a essas necessidades mais amplas.)

Mito: SASE permite que você permaneça com sua arquitetura de rede atual

O SASE pode ser eficaz apenas quando suas políticas e aplicação estão na borda, perto de onde seus usuários, dispositivos e aplicações se encontram. Esta proximidade é o que dá ao SASE suas características de segurança dinâmicas e fornece o desempenho e a confiabilidade que os usuários precisam para serem mais produtivos (e menos frustrados!).

Mito: SASE não precisa ver todo o tráfego da sua rede

O SASE é eficaz precisamente porque é uma abordagem completa à segurança. Seu poder, simplicidade e impacto são alimentados por sua capacidade de desenvolver contexto sobre usuários, dados e aplicações,

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

incluindo APIs subjacentes. O SASE prospera com a visibilidade. Este rico contexto é precisamente o que torna o SASE tão eficaz em um ambiente que oferece muito menos pontos de controle do que o antigo data center.

Mito: SASE aumenta a complexidade

A complexidade é a ruína de toda a segurança ou da existência de cada pessoa na rede, e é o denominador comum entre a maioria das falhas de segurança que chamam a atenção nas manchetes. O SASE exige que cada peça de segurança na sua rede trabalhe em harmonia. A segurança de rede estabelecida aos poucos nunca pode cumprir a visão do SASE de uma arquitetura de segurança em nuvem única e integrada na qual a política e sua aplicação são perfeitamente orquestradas e adaptáveis a requisitos em rápida mudança.

Mito: SASE precisa começar com a rede usando SD-WAN

Como um avanço na tecnologia de rede, a WAN definida por software (SD-WAN) pode simplificar muito o gerenciamento e a operação de uma rede de longa distância (WAN) e ser uma opção útil, e mais econômica, contra tecnologias de conectividade legadas como Multiprotocol Label Switching (MPLS). A utilidade da SD-WAN não deve ser descartada; nem deve sua relevância como um bloco de construção SASE ser ignorada. No entanto, muitos fornecedores que estão focados em SD-WAN já deram um salto de marketing para "SD-WAN, a maneira certa de chegar ao SASE" – uma alegação intelectualmente desonesta na melhor das hipóteses. SD-WAN – e firewalls, por falar nisso – não são o único caminho para o SASE, e não são nem mesmo os elementos mais básicos.

Mito: SASE não precisa de um novo ecossistema de fornecedores

É quase impossível para as empresas se livrarem totalmente de seu passado – produtos, tendências, crenças e investimentos antigos. Empresas com histórico de aquisição de outras empresas e tecnologias, e que construíram profundos poços de conhecimento institucional que são vistos como ativos significativos, relutam para se livrar desses fardos. SASE é uma nova abordagem para rede e segurança. Você não construirá para o futuro se você (ou seus fornecedores) tentar encaixar as soluções de ontem nas necessidades de amanhã.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

NESTE CAPÍTULO

- Compreendendo o que sua segurança precisa para se tornar nativa na nuvem
- Identificando como SASE cria uma segurança adequada para a nuvem
- Compreendendo porque o NG SWG é um elemento fundamental para o verdadeiro SASE
- Observando o NG SWG em ação

Capítulo 2
Reconhecendo a Importância do Next Generation Secure Web Gateway

Até recentemente, grande parte da estratégia de segurança se concentrava nas ameaças da web. Isso faz sentido. Antes de os serviços em nuvem serem adotados, o tráfego da web e os links da web em e-mails eram a principal fonte de ameaças digitais. As táticas dos departamentos de segurança – junto com os appliances amplamente usados, como os tradicionais proxies (SWGs), filtros da web e dispositivos proxy comumente encontrados em redes corporativas – foram todos ajustados para a frequência da web.

Essa abordagem também fazia sentido na época em que a maioria dos funcionários trabalhava em prédios corporativos e se conectava a recursos e à Internet usando as redes da empresa. Hoje, no entanto, quando seus usuários estão "no trabalho", eles geralmente estão remotos, móveis, movendo-se entre redes diferentes e realizando tarefas usando a nuvem. As pessoas usam uma ampla variedade de dispositivos ao

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

trabalhar em casa, passam um tempo produtivo em sua cafeteria favorita, visitam clientes e viajam. Tudo isso resulta em uma força de trabalho dinâmica que se conecta a redes, aplicações e dados distribuídos em todos os lugares, o tempo todo.

A era da nuvem claramente requer segurança aprimorada. Mas se você já esteve na fila de um aeroporto, sabe que aumentar a segurança nem sempre significa uma melhor segurança e não garante uma experiência ideal aos usuários. No aeroporto, o TSA PreCheck e os programas conceituados para viajantes ajudam a acelerar os procedimentos para passageiros em seus voos. Aspectos significativos dos procedimentos de segurança mudaram de oficiais de segurança e outros gargalos no aeroporto para um processo de verificação que começa antes que o passageiro chegue ao aeroporto. A intenção é aprimorar a experiência dos passageiros e garantir uma segurança adequada e maior eficiência a todo o sistema.

Um next generation SWG (NG SWG) é uma etapa importante em direção ao secure access service edge (SASE) e é cada vez mais adotado como a primeira etapa, porque leva você mais longe e garante maior maturidade na jornada SASE de forma muito rápida.

Livrando-se do Antigo

Seguindo o mesmo padrão que o setor de viagens adotou para viajantes frequentes, o setor de segurança teve que reconsiderar como e onde fornecer segurança aprimorada. Os appliances de gerações anteriores de segurança foram projetados para proteger redes e data centers, não aplicações em nuvem. Nem foram projetados para oferecer a flexibilidade e capacidade de resposta que os usuários esperam em uma experiência em nuvem.

Essa incompatibilidade – a tentativa de usar appliances antigos para novos cenários – levou a configurações de segurança dolorosas e excessivamente complexas que resultam em usuários frustrados, perda de produtividade, erros dolorosos e respostas lentas a violações de segurança. As ferramentas da geração anterior não se adaptam à natureza mutante do trabalho na nuvem.

Aqui está um exemplo de como essa incompatibilidade afeta a segurança e ilustra por que SASE é fundamental hoje: Com a abordagem antiga, os sistemas de segurança verificam quando o navegador do usuário faz conexões com os servidores da web. A análise de segurança não vai além da verificação de uma lista para determinar se uma URL é boa ou ruim. (O Capítulo 1 descreve isso como uma zona de defesa.)

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

Esse é um grande problema para qualquer pessoa que esteja protegendo a nuvem para sua empresa. Um dos desafios de segurança que mais cresce são as violações ocorrendo *dentro* dessas conexões aprovadas (ou seja, *depois* que você diz ok para uma URL). Os invasores apresentam formas aparentemente legítimas para coletar informações em um aplicação de software como serviço (SaaS) ou serviço em nuvem comprometidos para induzir seus usuários a fornecer dados preciosos e credenciais de login. Às vezes, os funcionários, com uma pressa compreensível para fazer as coisas rapidamente, recortam, copiam, colam, compartilham e transferem dados confidenciais para lugares onde sua organização não deseja. Uma zona de defesa não fornece mais proteção adequada neste ambiente.

O rápido aumento da importância dos serviços em nuvem para as empresas e o número crescente de funcionários remotos significa que você deve desenvolver e adotar novas abordagens, incluindo SASE. Sua empresa dependente da nuvem requer uma segurança que pode acompanhar permutações quase infinitas de localização, dispositivo e identidade do usuário. O objetivo é acelerar com segurança os usuários no caminho para interações altamente produtivas com as aplicações que eles usam para fazer seus trabalhos.

A necessidade de ampla visibilidade

Vamos sair do aeroporto e pegar a rodovia. Essa abordagem modulada pela web atua como um oficial de tráfego parado em uma interseção onde sua rede encontra o mundo exterior. O policial vigilante mantém um olhar atento sobre os veículos que passam, impedindo os motoristas de fazer coonversões em locais proibidos e procurando por veículos suspeitos.

Mas em um mundo dominado pela nuvem, o oficial enfrenta dois problemas significativos:

- A menos que o policial tenha sido instruído a procurar um veículo específico ou se um motorista se comportar mal claramente, ele não tem muitas informações para agir.
- Os sistemas de segurança cibernética pré-nuvem consideram apenas uma via de tráfego: o tráfego da web. Esses sistemas não conseguem ver as novas vias para SaaS, serviços baseados em nuvem e aplicações personalizadas – as mesmas vias usadas por cibercriminosos que conhecem essas vias, provavelmente não estão sendo inspecionadas. O policial não consegue ver os carros e caminhões passando por essas novas vias, veículos que poderiam estar escondendo uma horda de diamantes roubados ou, mais precisamente, seus preciosos dados.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

LEMBRETE

A verdadeira visibilidade significa ter a capacidade de ver as camadas mais finas de atividade e interação entre o usuário, dados e aplicações. Você precisa saber o que seus usuários estão fazendo dentro dessas aplicações – continuamente. O seu usuário está tentando colar dados confidenciais na aplicação SaaS? Ele está prestes a expor seu arquivo de folha de pagamento a um serviço de nuvem pública? Seus sistemas de segurança precisam saber.

Além da visibilidade: A vasta coleção de dados fornece um contexto rico

Na era da nuvem, a visibilidade por si só não é suficiente. Você poderia ter a imagem de mais alta resolução de algo e ainda assim perder os detalhes do que está naquela imagem se não souber como e onde procurar ou o que está realmente procurando. As equipes de segurança precisam desse detalhe para responder a perguntas como as seguintes:

- Quem é o usuário?
- Qual dispositivo ele está usando?
- Em qual rede o usuário está?
- Quais aplicações ele está acessando?
- O que pode ser conhecido sobre cada aplicação e seu comportamento?
- Quais dados o usuário está acessando?
- Seus comportamentos atuais e passados são consistentes?

Nos referimos aos detalhes dentro da imagem como *contexto*, que é um dos conceitos mais fundamentais no acesso à nuvem. Esse contexto é o que torna possível definir e aplicar políticas de segurança que podem limitar o que acontece conforme necessário em ações e aplicações em tempo real. (Veja o capítulo 4 para obter mais informações sobre contexto e políticas.)

LEMBRETE

Os requisitos para uma segurança eficaz na era da nuvem são os seguintes:

- Minimizar a complexidade de sua arquitetura de segurança para tornar o trabalho mais fácil para os usuários e para a equipe de segurança
- Fornecer aos usuários – não importa onde eles estejam – interações rápidas e responsivas com suas aplicações para que possam obter todos os benefícios da nuvem

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

- Gerenciar riscos para o seu negócio continuamente, sendo capaz de ver facilmente e lidar rapidamente com atividades potencialmente arriscadas envolvendo dados da empresa e usuários

Uma arquitetura SASE devidamente implementada faz tudo isso.

SASE: Construída para a nuvem

Você não pode simplesmente renomear ou reaproveitar a tecnologia de ontem e pensar que ela estará pronta para o trabalho de segurança em nuvem de hoje, muito menos para o de amanhã. Os appliances legados não são restritos apenas pelo fato de ficarem presos em seu data center. A nuvem também funciona em uma escala e velocidade totalmente diferentes. Os serviços de segurança precisam ser projetados para operar na mesma velocidade e escala.

O que torna o SASE uma estrutura de segurança tão atraente é que, assim como a nuvem, ele torna o trabalho mais fácil e flexível.

Ser construído para a nuvem significa que todos os requisitos básicos de SASE devem ser incorporados ao design da arquitetura. Para realizar o trabalho rapidamente e em escala, a verdadeira arquitetura SASE exige que todos os serviços envolvidos na segurança façam seu trabalho em coordenação, como uma ação rápida e contínua. Toda a sua verificação e inspeção tem que acontecer "lá fora", onde quer que seja. O tráfego de um usuário não precisa retornar um gargalo de segurança (seu data center!) para cada interação. Ao trazer a segurança para perto do usuário e dos pontos de acesso, cada interação se torna mais segura e mais eficiente. Sua segurança está alinhada com tudo que a nuvem deve ser. Voltando à metáfora da rodovia, com SASE, o policial agora finalmente vê todas as vias de tráfego.

Facilitando a Verdadeira Segurança em Nuvem

SASE, bem feita, tem duas funções principais:

- **Fornecer uma rede de borda global que concede a seus usuários acesso a serviços em nuvem, não importa onde esses usuários estejam:** Essa rede de borda global autentica usuários e, em seguida, otimiza suas conexões em direção a aplicações SaaS, seu data center e outros serviços.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

» **Fornecer serviços de segurança em toda a rede de borda global para que estejam próximos dos usuários:** Isso garante que usuários e organizações possam sempre contar com essa rede de proteção para realizar o trabalho com segurança. Essa configuração também torna viável aplicar políticas de segurança e ditar as interações online dos usuários com base em quem a pessoa é e onde ela está, e fazer isso enquanto otimiza a segurança, a confiabilidade e o desempenho dessas atividades.

LEMBRETE

A arquitetura SASE implementada corretamente é eficaz porque reconhece que as aplicações e as cargas de trabalho foram movidas para a nuvem e, portanto, os serviços de segurança devem segui-lo. Para os seus usuários, isso significa que eles não precisam se preocupar em passar por obstáculos para usar uma aplicação. Quando eles vão a uma cafeteria, ter acesso ao que precisam é tão fácil quanto pedir um café com leite. Para você, o profissional de segurança, ter contexto e serviços de segurança integrados e compartilhados possibilita a criação de políticas sofisticadas que podem ser aplicadas automática e apropriadamente com base em quem precisa de acesso, o que ele está tentando acessar e onde todas as peças da interação estão localizadas. Em um mundo digital que deixou os limites restritivos do data center para as possibilidades abertas da nuvem, SASE é a *única* arquitetura de segurança e redes que faz sentido.

E quanto ao data center?

O data center ainda tem uma função a desempenhar na TI corporativa em um futuro próximo. Grandes aplicações, como planejamento de recursos empresariais (ERP), foram desenvolvidas para durar décadas, portanto, essas aplicações na nuvem privada provavelmente coexistirão com o SaaS e a nuvem pública por um longo tempo. De forma mais ampla, as organizações investiram muito ao longo dos anos para criar e alimentar seus data centers corporativos. Deixar de lado essa dinâmica pode ser difícil. Seja paciente.

LEMBRETE

Quando você aceita o data center como apenas um dos muitos lugares que seus usuários vão para realizar seus trabalhos, rotear todo o tráfego vinculado à nuvem através dele começa a fazer menos sentido. Forçar o tráfego de um usuário a desviar constantemente através da rede privada de sua organização para, então, ser processado por uma sucessão de caixas pretas de segurança separadas – um processo conhecido pelos profissionais de segurança como *hairpinning* ou *backhauling* – é complicado e ineficiente. Afinal, você não planejaria dirigir de Los Angeles a San

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

Francisco passando pelo Cairo, a menos que tivesse muito tempo livre (e um navio). A mesma lógica se aplica à vinculação de seus usuários às suas aplicações SaaS.

DICA

SASE não trata apenas de aplicações SaaS. Ele pode e deve ser usado para fornecer acesso e proteger todos as suas aplicações, incluindo as do data center, independentemente de o usuário estar dentro ou fora do local.

Os serviços certos para cada cenário

A flexibilidade é uma das grandes vantagens dos serviços em nuvem. Mas apenas introduzir palavras como *nuvem* ou *SASE* em um produto não levará você até lá. A flexibilidade deve ser projetada intencionalmente em uma verdadeira implementação SASE. Como o contexto na nuvem muda constantemente, diferentes tecnologias e serviços serão necessários para trabalhar juntos de modo específico e aplicados conforme os cenários mudam e evoluem. Feita corretamente, a implementação de SASE aplica todos os serviços de segurança necessários para fazer cumprir a política de segurança para qualquer conexão, sempre priorizando os seguintes objetivos:

- Acomodar uma força de trabalho distribuída
- Otimizar os níveis de serviço com base na mudança de contexto
- Manter os serviços de segurança o mais próximo possível do usuário em todos os momentos
- Fornecer serviços de segurança necessários para operar em hiperescala com o desempenho necessário para fluxos de trabalho empresariais modernos

Então, a questão agora é: como mudar sua organização para um projeto SASE eficaz? Nas seções a seguir, daremos uma olhada em alguns requisitos fundamentais – incluindo um muito importante, o NG SWG.

Precisando de uma Rede de Borda Global

Quando analisada através das lentes de arquiteturas de segurança antigas, a própria ideia de proteger a nuvem para os negócios parece conter uma contradição. Por um lado, você tem usuários que contam com você para fornecer acesso rápido às suas aplicações e dados, de qualquer lugar, com o mínimo de interrupção de bloqueios de segurança. Isso está em oposição quase perfeita à expectativa de que você também forneça a seus usuários e empresas o máximo em segurança e proteção de dados.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

Realizar o hairpinning do tráfego em seu data center não era um problema significativo quando 85% dos usuários trabalhavam em escritórios corporativos. No mundo criado pela pandemia da COVID-19, mais trabalhadores experimentaram trabalhar em casa e 74% dos trabalhadores agora gostariam de trabalhar em casa pelo menos dois dias por semana, de acordo com uma pesquisa da PwC. Para usuários remotos, o hairpinning introduz uma latência e obstáculos que atrapalham uma experiência produtiva ao usuário. Como o trabalho remoto é provavelmente o novo normal, é imperativo que a segurança mude para a nuvem, onde possa acompanhar melhor os usuários e fornecer proteção de dados sem degradar a experiência do usuário.

Essa última parte é importante porque usuários frustrados que desejam acesso rápido evitarão se conectar à sua rede privada virtual (VPN), algo que já fazem há anos. Quando isso acontece, seus usuários e dados não estão protegidos de forma alguma, e sua equipe de segurança está trabalhando às cegas. Uma rede de borda global possibilita que os usuários se conectem à nuvem de qualquer lugar, sem ter que voltar ao data center para ter proteção e segurança de dados.

LEMBRETE

Ter acesso a uma rede de borda global é uma vantagem distinta para sua força de trabalho móvel. A rede de borda global da Netskope fornece pontos de acesso em mais de 40 regiões ao redor do mundo onde as funções de segurança são hospedadas e executadas. Isso é o que torna possível manter a segurança perto do usuário em todos os momentos e entregar uma inspeção de passagem única do tráfego (consulte "Inspeção de passagem única", mais adiante neste capítulo, para saber mais – por enquanto, pense apenas em "rápido "). Juntos, eles ajudam a fornecer uma experiência de usuário tranquila, rápida e segura.

Uma das diferenças fundamentais entre SASE e a segurança tradicional é como e onde a segurança é aplicada. Em uma arquitetura de segurança SASE, quando um usuário deseja se conectar à Internet – seja para usar uma aplicação SaaS, navegar na web ou publicar algo em uma rede social – ele primeiro se conecta a um ponto de acesso na rede de borda global. Cada ponto de acesso inclui os recursos computacionais necessários para alimentar os serviços de segurança. Por causa dessa distribuição, os usuários não se deparam com as implicações de desempenho ou as complexas dores de cabeça com a segurança em várias etapas que encontraram quando tudo fluía pelo data center corporativo.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

Compreendendo como o NG SWG se relaciona com SASE

A forma completa e ideal de SASE é uma nova arquitetura de segurança na qual todos os seus serviços de segurança trabalham juntos em perfeita coordenação. Se isso soa como um grande empreendimento, de fato é. Mas você não precisa fazer tudo imediatamente. Ao dar os primeiros passos corretos, você criará uma base sólida para tudo o que vem depois. Uma etapa inicial importante é implementar o NG SWG. É um diferenciador crítico entre "fingir ser SASE" e ser um projeto SASE executado corretamente. NG SWG é o catalisador para a criação da nuvem de segurança que torna SASE possível.

SASE é melhor quando implementada usando uma arquitetura de *microsserviços*. Simplificando, microsserviços são uma maneira de construir um sistema a partir de muitos módulos de serviços pequenos e discretos. Quando bem feitos, esses módulos compartilham uma base de código comum e todos trabalham juntos para entender a linguagem nativa da nuvem.

Todos esses serviços devem ser orquestrados para funcionarem juntos para fazer cumprir suas políticas de segurança com base no conteúdo e no contexto. O NG SWG atua como o controle de tráfego aéreo de uma implementação SASE. Em qualquer lugar e em qualquer momento que um usuário acesse os dados, o NG SWG coordena os serviços para que atuem em conjunto para aplicar as políticas de segurança em todo o ambiente de TI.

Em uma sequência rápida, o NG SWG aplica todos os serviços de segurança compartilhados necessários para a aplicação de segurança baseada em políticas para cada conexão com base em uma compreensão extremamente rica dos usuários, dados, aplicações e tráfego em sua rede.

O NG SWG também permite que você desative appliances menos capazes, reduzindo a complexidade de sua infraestrutura de segurança sem abrir mão das características de seus melhores e mais úteis serviços. Agora parte do NG SWG, esses serviços são aplicados em coordenação com os muitos novos serviços que trabalham juntos para inspecionar profundamente o seu SaaS e o tráfego da web, obter essa compreensão super rica e aplicar políticas de segurança baseadas em contexto.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

ATENÇÃO

Uma plataforma de nuvem pública genérica como Amazon Web Services (AWS) ou Google Cloud não é SASE, ou nem mesmo pronta para SASE, por conta própria. As soluções de nuvem pública são otimizadas para fornecer aplicações – a arquitetura de nuvem pública é projetada como um destino, e não como um hub para serviços de segurança através do qual o tráfego flui em seu caminho para outro lugar. SASE tem requisitos de computação e desempenho exclusivos que tornam possível oferecer suporte a uma arquitetura baseada em microsserviços projetada para cargas de trabalho de segurança.

Proxy versus NG SWG

Proxies (SWGs) às vezes são chamados de gateways de Internet ou web proxies ou filtros da web seguros (ou outros nomes). Eles existem de alguma forma desde pelo menos os anos 90 e foram originalmente construídos em uma era muito diferente de hoje.

O que torna o NG SWG diferente do proxy tradicional e de outros produtos semelhantes com os quais você pode estar familiarizado? A resposta mais simples é que o proxy tradicional aborda apenas o tráfego da web e fornece apenas controles de permissão/negação. Ele foi construído para uma época em que a Internet girava em torno de sites e comunicação de Hypertext Transfer Protocol/Secure (HTTP/S) – ao modo "Sim, você pode acesse este site" ou "Não, você definitivamente não pode acessar, hum-hum, *este* site."

O NG SWG, no entanto, é o guarda-chuva organizador sob o qual toda a web e outros serviços residem, ao mesmo tempo em que também cria uma nuvem de segurança expansiva com pontos de controle próximos ao usuário (aquela rede de borda global anterior) onde uma ampla gama de serviços de segurança é orquestrada. O NG SWG executa e aprimora todas as funções básicas de tráfego da web em proxies legados e appliances semelhantes e adiciona novas funções de segurança significativas. Em particular, o NG SWG realiza uma inspeção profunda do tráfego da web e da nuvem, procurando ver o que está acontecendo nas interações, aplicando proteção de dados e contra ameaças e construindo uma compreensão do conteúdo e do contexto para impor controles de política granulares.

Com o NG SWG em seu projeto SASE, o policial ou controlador de trânsito pode ver todas as vias de tráfego, saber o que está acontecendo dentro dos veículos e fazer cumprir as regras (consulte a tabela 2-1).

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

TABELA 2-1 **Como a Netskope Atende aos Requisitos SASE**

Requisito SASE	NG SWG da Netskope
Nativo na nuvem com arquitetura de passagem única para inspeção de tráfego criptografada	Reside inteiramente na nuvem usando arquitetura nativa na nuvem com a capacidade de decodificar e entender aplicações e serviços em nuvem para o contexto de dados. A arquitetura de passagem única da Netskope fornece dados avançados e inspeção de ameaças de tráfego criptografado (suporte para TLS1.3 sem conexão de negociação descendente) na velocidade da linha em cada data center NewEdge para todos os serviços (proxy, agente de segurança de acesso à nuvem [CASB], prevenção avançada de perda de dados [DLP], sandbox, análise de aprendizado de máquina [ML], firewall como serviço [FWaaS], remote browser isolation [RBI] e assim por diante).
Pontos de presença, com acordos de nível de serviço (SLAs) para baixa latência e alta disponibilidade	A Netskope NewEdge Network, uma nuvem privada de segurança de alto desempenho, hospeda serviços de segurança e fornece abundantes pontos de acesso em todo o mundo. Com baixa latência de um dígito de milissegundos para obter a melhor experiência, a NewEdge é apoiada por cinco noves (99,999%) de disponibilidade de SLA de serviços inline, além do Trust Portal para serviço em tempo real/status do data center (`https://trust.netskope.com`).
Segurança como serviços por meio de um único plano de controle de política	Plataforma de uma só nuvem e mecanismo de política executados em planos de gerenciamento, separados dos planos de dados de processamento de tráfego. Um único console é usado para facilitar a administração para gerenciar e adicionar quaisquer serviços de segurança SASE, que são implantados por meio de um único agente para acesso simplificado e experiência do usuário em todos os locais.
Inspeção de tráfego com proxy de encaminhamento NG SWG de cinco tipos de tráfego de usuário	Analisa todas as vias de tráfego do usuário para web, SaaS gerenciado, aplicações de shadow IT, serviços de nuvem pública e aplicações personalizadas na nuvem pública ou data center, ao contrário de proxies legados que analisam apenas o tráfego da web. Políticas de inspeção de segurança consistentes são aplicadas em todos os métodos de acesso.
Visibilidade e controle de dados confidenciais e DLP em nuvem	Visibilidade incomparável em web, SaaS, shadow IT, serviços de nuvem pública e aplicações personalizadas em nuvem pública para movimentação de dados confidenciais. Protege os dados em movimento para cinco tipos de tráfego de usuário mais DLP de e-mail para o tráfego de saída do Microsoft Office 365 (M365) e do Gmail Simple Mail Transfer Protocol (SMTP); a chave para esse recurso é analisar a movimentação de dados entre aplicações pessoais e corporativas e instâncias de aplicações, bem como anomalias na movimentação de dados.

(continua)

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

TABELA 2-1 *(continua)*

Requisito SASE	NG SWG da Netskope
Proteção avançada contra ameaças (ATP) e análise de comportamento de usuários e entidades (UEBA)	Oferece proteção contra malware habilitado para web e nuvem, phishing em nuvem e documentos maliciosos com antimalware inline, análise pré-execução, sandbox, análise de aprendizado de máquina e UEBA para anomalias de comportamento e pontuação de risco do usuário com análises em tempo real e visualização do painel em todos os usuários e aplicações para dados, ameaças e atividades.
Firewall de nuvem	Fornece controles de firewall de nuvem de saída para usuários remotos e filiais em todas as portas e protocolos.
RBI	O pixel RBI direcionado renderiza sites arriscados e não categorizados para fornecer acesso seguro aos usuários, além de bloquear downloads e uploads de arquivos e entradas de formulários vistos como ataques de phishing e copiar/colar na área de transferência.
Postura de segurança de rede zero trust	Controles de segurança de confiança zero (zero trust) aplicados a partir do acesso do usuário (acesso de rede de confiança zero [ZTNA], gerenciamento de identidades e acessos [IAM]) para capturar informações de risco e contexto para usuário, tipo de dispositivo, aplicação, instância de aplicação, classificação de risco de aplicação, categoria, atividade, conteúdo e ação para aplicar controles de política condicionais e contextuais baseados em risco. Conforme o comportamento e as anomalias do usuário são monitorados, as ações de política adaptativa são aplicadas dinamicamente de acordo com os princípios de Confiança Zero, incluindo desafios de autenticação progressiva, limitação do acesso à atividade, movimentação de dados ou encerramento do acesso à aplicação do usuário.
Criação de política orientada ao contexto adaptável e aplicação consistente	Fornece treinamento em tempo real, autenticação progressiva e políticas adaptáveis com base no risco da aplicação, risco do usuário e contexto de dados. A implementação em tempo real é consistente em todos os usuários, filiais e outros locais de presença.
IAM	Integra-se com IAM e sistemas de provedor de identidade que gerenciam e verificam a identidade digital de usuários e grupos.
Proteção de endpoint	Ativa o compartilhamento bidirecional de indicador automatizado de comprometimento (IOC), bem como o acesso condicional com ativação de proteção de endpoint e a capacidade de compartilhar metadados avançados para investigações.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

Requisito SASE	NG SWG da Netskope
Informações de segurança e gerenciamento de eventos (SIEM) e centro de operações de segurança (SOC)	Fornece compartilhamento de IOC e metadados avançados para funcionar perfeitamente com os pontos de gerenciamento e painéis usados pela equipe de segurança para investigar alertas e incidentes.
Análise e visualização em tempo real	Fornece metadados de nuvem para visualização e análise em tempo real sobre movimentação de dados, ameaças, usuários e aplicações em painéis personalizáveis dinâmicos para equipes em nível executivo, nível de diretoria e de segurança e risco.

Um pouco de SASE versus SASE implementado corretamente

Com o NG SWG, você não precisa mais configurar centenas ou milhares de regras minúsculas, detalhadas, porém complicadas, separadamente para cada uma de suas soluções e appliances de segurança, cada um dos quais lida com apenas uma pequena parte do tráfego em seu data center. Nas melhores soluções SASE da indústria usando NG SWG, você se concentra na criação de políticas de alto nível que descrevem os resultados desejados para *todo* o tráfego. O NG SWG então diz aos diferentes serviços de segurança o que fazer para entregar esses resultados em seu tráfego da web, aplicações SaaS gerenciadas, aplicações SaaS não gerenciadas (shadow IT), serviços de nuvem pública e aplicações personalizadas hospedadas na nuvem pública. A aplicação pode até incluir recursos avançados, como treinamento do usuário e ações baseadas em risco para permitir respostas diferenciadas e apropriadas. Você define as coisas que deseja que aconteçam em toda a arquitetura, e o NG SWG coordena os serviços para que isso aconteça.

MATERIAL TÉCNICO

Como o NG SWG cria a base fundamentada em contexto para a implementação adequada do SASE? A tabela 2-1 (anteriormente neste capítulo) mostra quais serviços e recursos de uma arquitetura SASE o NG SWG oferece. Ele também descreve os outros serviços que ajudam a completar a imagem SASE quando conectados ao NG SWG da Netskope.

Examinando como um NG SWG funciona

A seção anterior descreve o que os NG SWGs oferecem dentro da arquitetura SASE mais ampla. Esta seção se aprofunda em como o NG SWG coloca isso em ação.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

LEMBRETE

Embora a descrição a seguir seja organizada em seções, lembre-se de que a segurança com NG SWG não é uma cadeia de dispositivos separados ou uma sequência linear de operações como você teria em um data center.

Inspeção de passagem única

Quando o dispositivo de um usuário é conectado a um ponto de acesso na rede de borda global, todo o tráfego do usuário passa por uma inspeção de passagem única. *Passagem única* é exatamente o que parece: todos os serviços de segurança necessários para fazer cumprir a política formam um funil contínuo através do qual o tráfego flui. O tráfego entre o usuário e o destino passa por esse funil único uma só vez, em tempo real. Esse processo é diferente dos appliances de proxy legados somente para web e das soluções de tráfego inline em nuvem, que eram como ter uma série de funis independentes pelos quais tudo tinha que passar.

A inspeção de passagem única do NG SWG se aplica ao conteúdo da web, aplicações SaaS gerenciadas por sua organização, qualquer aplicação SaaS de shadow IT ou não gerenciada que um usuário tente usar, serviços de nuvem pública e qualquer aplicação personalizada na nuvem pública que sua organização implemente. O tráfego da web e da nuvem flui por meio desse sistema único, que agrega e coordena todos os serviços de segurança como uma plataforma única e coerente e, em seguida, os aprimora para dar vida ao SASE devidamente implementado.

O tráfego é filtrado, em uma única passagem, em etapas. Os problemas mais óbvios são removidos primeiro, deixando uma quantidade cada vez menor de tráfego para ser submetida a uma análise mais detalhada (consulte o capítulo 4 para saber mais sobre esses estágios).

Quanto mais rico for o contexto, mais forte será a segurança

O contexto é a chave para a segurança ativa, profundamente inspecionada e ágil oferecida por SASE quando implementado corretamente. No instante em que um usuário se conecta a um ponto de acesso, os serviços NG SWG dentro da nuvem de segurança desenvolvem uma imagem contextual disponível para todos os serviços. Essa imagem é usada para ditar como a política é aplicada. Este contexto é um grande conglomerado de *metadados* (dados que descrevem outros dados ou adicionam contexto), incluindo uma riqueza de informações que identificam e reconhecem:

- O usuário ou grupo organizacional ao qual o usuário pertence
- O dispositivo do usuário, sua localização e se esse dispositivo é gerenciado por sua organização

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

- O site, aplicação ou pacote de aplicações com o qual o usuário está trabalhando
- Cloud Confidence Index da Netskope – uma classificação de risco derivada de vários serviços de avaliação de segurança independentes e atribuída ao site, aplicação ou pacote de aplicações específico que está sendo acessado
- Os dados solicitados, gerados e/ou usados pelo usuário e pela aplicação

Além disso, este contexto é aprimorado com muitas fontes novas e variadas de informações que o NG SWG pode aproveitar para adicionar mais detalhes com base em:

- Consciência do comportamento do usuário e quaisquer anomalias nesse comportamento
- Inspeção do conteúdo e dos dados contidos no tráfego
- Atividades realizadas pela aplicação, conteúdo da web e serviços acessados e a natureza dessas atividades
- Conhecimento dos dados dentro do ambiente da aplicação
- Informações armazenadas coletadas em interações anteriores

O contexto muda constantemente durante todo o tempo em que o usuário tem acesso. Você deseja um sistema ágil, responsivo e adequado às variações sutis de risco apresentadas por diferentes combinações de detalhes contextuais. A política pode descrever o resultado de segurança desejado, mas o contexto determina a combinação ideal de serviços e ações de segurança que entregam esse resultado com base nas particularidades do momento. Por exemplo, um usuário que repentinamente está agindo estranhamente e acessando arquivos para os quais não deveria, está sujeito à *autenticação step-up*, um pedido de mais informações para estabelecer a sua identidade. Ter um contexto dinâmico enorme torna possível aplicar políticas de segurança granulares e habilitar ações de política em tempo real conforme o contexto muda. Inteligência artificial (IA) e ML desempenham um papel importante em ajudar sua segurança a filtrar esses detalhes contextuais diferenciados (consulte o capítulo 4).

LEMBRETE

A segurança da web legada era basicamente uma proposição de "sim ou não". O NG SWG é uma abordagem dinâmica e contínua à segurança que observa continuamente o comportamento e o que está acontecendo dentro de todo o tráfego da web e da nuvem. Isso dá ao NG SWG o poder de ajustar decisões sobre segurança em tempo real, um recurso que é fundamental para proteger a interação do usuário com aplicações e sites.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

MATERIAL TÉCNICO

A tabela 2-2 descreve alguns dos serviços de segurança que são expandidos e aprimorados pelo NG SWG e que estabelecem a base para uma arquitetura SASE completa.

TABELA 2-2 Serviços de Segurança Essenciais Fornecidos pelo NG SWG

Serviço de segurança	O que o serviço fazia em uma configuração tradicional	Como o NG SWG maximiza o serviço
SWG	Protegia os usuários contra ameaças da web e conteúdo questionável.	Adiciona contexto às aplicações e dados (quem está usando a aplicação ou dados, onde está usando e por quê). Adiciona proteção aos dados (evitando sua modificação ou roubo). Impede o uso impróprio de dados (evitando que os dados sejam usados ou enviados para onde não se destinam).
DLP	Protegia apenas os dados armazenados no data center e os que estão sendo movidos além do firewall do data center pela web.	Protege todos os dados em movimento, incluindo dados distribuídos na web, em aplicações SaaS, na nuvem, em serviços em nuvem e em aplicações personalizadas na nuvem pública.
CASB	Aplicações gerenciadas monitoradas e protegidas que forneciam interfaces de programação de aplicações (APIs) visíveis que podiam ser monitoradas e protegidas por meio dessas APIs e também inline; seu foco estava nos dados em repouso e nos dados em movimento – dados armazenados no ambiente da aplicação ou no data center, além dos transmitidos entre os dois; nem todas as soluções suportavam todas as modalidades.	Monitora aplicações não gerenciadas que não oferecem APIs de gerenciamento evidentes, permitindo que um grande número de aplicações não gerenciadas sejam monitoradas e protegidas. Monitora dados em movimento; os dados que estão sendo usados ativamente e transmitidos a aplicações e sites podem ser protegidos. Oferece ricas informações sobre risco de aplicações para informar a seleção e implantação de SaaS.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

Serviço de segurança	O que o serviço fazia em uma configuração tradicional	Como o NG SWG maximiza o serviço
Proteção avançada contra ameaças (ATP)	Protegia contra ameaças baseadas na web usando métodos avançados, como *sandbox* (detonando executáveis com segurança para detectar intenções maliciosas e hiperlinks) e inteligência contra ameaças (IOCs compartilhados de fontes públicas e pagas).	Protege contra ameaças habilitadas para nuvem, incluindo entrega de malware e ataques de phishing usando aplicações e serviços em nuvem, como Microsoft Office 365 e Google Docs. Isola aplicações e sites desconhecidos para interagir com segurança e proteger contra ameaças potenciais.

Aplicação de política de passagem única

É claro que mesmo o contexto mais detalhado não ajuda muito, a menos que seus usuários e serviços de segurança saibam o que devem e o que não devem fazer. Você precisa de regras básicas com as quais o contexto possa ser comparado.

Você pode ter escrito um conjunto de regras que ditariam o comportamento do firewall, verificando a entrada de URL feita por um usuário em relação às listas de sites que você decidiu bloquear. Mas a segurança tradicional sempre impõe comprometimentos entre velocidade e flexibilidade, de um lado, e segurança, do outro. Entre a inundação constante de novos sites e mudanças de pessoal ao longo do tempo, sua lista de regras pode se tornar enorme – e frágil. Você pode ter medo de mudar suas regras – talvez para permitir o acesso a uma ferramenta de vendas útil – por medo de abrir inadvertidamente uma nova vulnerabilidade.

Um projeto SASE, feito da maneira certa, acaba com essas desvantagens, oferecendo um novo paradigma para fornecer segurança de nível mundial. A aplicação de política de passagem única é o poder, ou superpoder, do SASE para fazer cumprir a política de dados ou controles de atividade em todas as aplicações, categorias de aplicações e serviços da web. Pense nisso como o poder do contexto em ação. Por exemplo, se a inspeção de passagem única detectar um tipo de dados confidenciais em um formulário da web ou dentro de um arquivo ou campo em um aplicação ou canal do Slack, a aplicação da política de passagem única pode bloquear o conteúdo na web e/ou controlar a atividade na aplicação (upload) enquanto permite a visualização.

Com uma estrutura de política consistente, granular e centralizada que se estende por todos os seus serviços de segurança, você pode assumir o controle e declarar sua intenção com clareza – sem se preocupar com

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

os detalhes de como implementar uma política específica. Isso reduz drasticamente a complexidade.

DICA

SASE com NG SWG muda o trabalho de sua equipe de segurança. Em vez de escrever códigos separados de maneira ineficiente para gerenciar cada dispositivo separado, sua equipe se concentra em escrever regras eficazes e de alto nível para fornecer serviços que façam sentido para os negócios.

NG SWG em ação

A figura 2-1 mostra como é o NG SWG em ação da perspectiva de um único usuário.

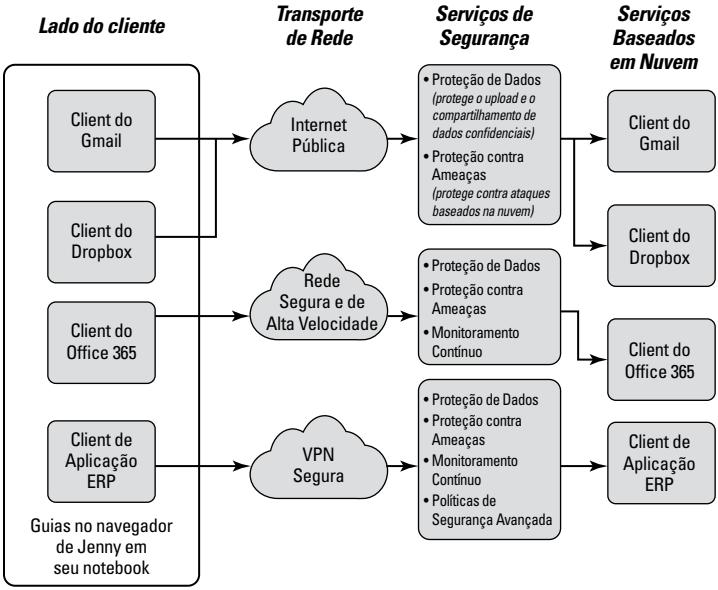

FIGURA 2-1: NG SWG em ação para uma única usuária chamada Jenny.

Na figura 2-1, Jenny representa uma usuária típica que trabalha em casa e que pode iniciar quatro conexões de seu notebook para:

- Sua conta pessoal do Gmail
- E-mail corporativo dela no Microsoft Office 365
- Uma aplicação de armazenamento em nuvem como Dropbox
- Aplicações essenciais gerenciadas pela empresa, como Salesforce, ServiceNow ou Workday

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

Nesse caso, o NG SWG lida com essas interações discretas da seguinte maneira:

- **A aplicação pessoal do Gmail de Jenny é roteada para a Internet pública.** O NG SWG protege e analisa a conexão, fornecendo proteção contra ameaças e proteção de dados, resultando em uma experiência de usuário de alto desempenho.
- **O e-mail corporativo no Microsoft Office 365 de Jenny é roteado por uma rede segura de alta velocidade.** O tráfego nesta conexão é monitorado continuamente para garantir que dados cruciais não sejam compartilhados.
- **A conexão com a aplicação de armazenamento em nuvem Dropbox não gerenciada é roteada pela Internet pública.** O NG SWG protege e analisa essa conexão continuamente e impõe a política de segurança, permitindo que Jenny visualize arquivos compartilhados de fontes de terceiros. No entanto, o NG SWG bloqueia os uploads e aplica a prevenção contra ameaças aos downloads de arquivo quando Jenny fornece uma justificativa para o download de arquivo.
- **A conexão de Jenny com a aplicação corporativa de uso essencial é roteada por uma VPN especial criptografada.** A conexão é monitorada por vários serviços de segurança diferentes que fornecem camadas de proteção para garantir que os dados não sejam compartilhados ou usados indevidamente. Isso também impõe políticas para garantir que a aplicação seja usada corretamente.

Neste exemplo, usando apenas um funcionário, você pode ver como quatro conexões diferentes são protegidas. Cada conexão tem um contexto distinto que dita a aplicação de políticas relevantes e específicas. A experiência do usuário resultante é excelente e o nível de segurança é alto. Jenny pode verificar seu Gmail pessoal e fazer seu trabalho sem arriscar os dados da empresa. Essa é a diferença que o NG SWG pode fazer.

Nesta conjuntura, é importante notar que o NG SWG não é a *única* diferença quando se trata de arquitetura SASE implementada corretamente. O NG SWG não é um feijão mágico; a funcionalidade CASB (encontrada não em proxy, mas no verdadeiro NG SWG) e a aplicação criteriosa dos princípios de confiança zero são outras peças-chave do quebra-cabeça.

No entanto, o NG SWG é uma grande peça. Ele pode acelerar drasticamente sua jornada para SASE e ajudá-lo a deixar para trás tecnologias antigas, como proxy legado, que só prejudicará o sucesso de sua arquitetura SASE.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

NESTE CAPÍTULO

- **Melhorando a segurança ao conhecer melhor sua equipe**
- **Explorando qual combinação de serviços torna a segurança mais robusta**
- **Compreendendo como a confiança muda quando as pessoas trabalham fora da rede que você tradicionalmente controla**
- **Descobrindo como a segurança é maximizada para proteger as pessoas na nuvem**

Capítulo 3
Protegendo Pessoas

Grande parte da segurança tem a ver com pessoas – proteger as pessoas que são importantes para você e proteger as coisas que são importantes para você de pessoas com más intenções. Para segurança corporativa e equipes de rede, os cenários óbvios e práticos são aqueles preocupados em proteger o pessoal e os ativos digitais de sua organização daqueles que poderiam causar danos, ao mesmo tempo em que garantem que seus funcionários e clientes tenham experiências boas e confiáveis.

Mas segurança também significa proteger sua equipe de si mesma – os erros, tentações, negligência e erros de julgamento que podem causar danos irreparáveis a eles ou à sua empresa. (Você pode se surpreender ao saber que mais de 90 por cento dos incidentes de segurança cibernética são atribuíveis a erro humano, de acordo com a Kaspersky Lab.)

O modelo secure access service edge (SASE), quando corretamente projetado, fornece à sua equipe de segurança as informações e ferramentas para enfrentar de forma eficaz e inteligente esses grandes desafios, ajudando sua organização em duas frentes:

- **Proteger seus sistemas contra pessoas que não estão autorizadas a acessá-los:** quer esses sistemas estejam em seu data center ou na nuvem, o mesmo padrão deve ser aplicado em todos os momentos.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

- **Quando pessoas estão autorizadas a entrar em seus sistemas, impedi-las de fazer coisas inseguras intencionalmente ou não**

SASE muda a segurança para um ambiente de nuvem baseado em borda criando uma estrutura que é rica em serviços de segurança, fornece total visibilidade e controle e pode chegar a qualquer lugar.

Este capítulo analisa como uma arquitetura SASE bem projetadaa, construída usando next gen secure web gateway (NG SWG), cloud access security broker (CASB) e princípios de zero trust (confiança zero), torna a vida mais segura e fácil quando seus usuários estão na nuvem.

Contexto: Mudando o Jogo a Favor da Segurança

Um SASE eficaz é orientado pelo contexto, e o gerador desse rico plano de fundo reside na plataforma Netskope. Criado pela Netskope, o Cloud XD (abreviação de extreme definition) é o serviço de contexto que transforma seu tráfego da web, serviços em nuvem e atividade de aplicação de software como serviço (SaaS) em uma visão inteligível e acionável. O Cloud XD captura e decodifica detalhes dentro do tráfego que torna possível identificar usuários, seus dispositivos, aplicações em uso e atividades específicas dentro dessas aplicações. Essas informações decodificadas são compartilhadas com todos os serviços de segurança, tornando possível aplicar políticas de segurança detalhadas com base nas dicas fornecidas pelo Cloud XD.

Respondendo a perguntas básicas

Os detalhes que o Cloud XD fornece são amplos e variados, dependendo da atividade específica em andamento. Esses detalhes podem incluir informações como:

- O usuário está enviando ou baixando algo?
- Em caso afirmativo, esse "algo" inclui dados confidenciais?
- Quantos bytes o usuário está enviando ou baixando?
- Qual aplicação está sendo usada?
- A pessoa está usando uma instância corporativa ou pessoal de uma aplicação?

Esses exemplos são simples, mas podem surpreendê-lo ao saber que, até recentemente, esses dados básicos de alto nível não estavam efetivamente disponíveis para as equipes de segurança, e nem perto de uma

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

apresentação agregada e coerente que pudesse ser aplicada em todo o cenário de segurança.

Esses detalhes recém-disponíveis tornam possível construir uma narrativa sobre a atividade de um usuário que pode soar mais ou menos assim:

> Lauren está usando sua instância corporativa do Gmail e recebeu acesso por meio de suas credenciais de login corporativas: um nome de usuário que você conhece, a senha dela que foi aceita e um código de autenticação de dois fatores (2FA) que foi aceito. Você sabe que Lauren pode ter uma conta pessoal do Gmail, portanto, você acompanhará em qual instância ela está trabalhando, pois o Gmail permite que ela alterne rapidamente entre contas na janela do navegador.

ATENÇÃO

O contexto, no sentido de segurança moderna e sofisticada, requer que seus serviços de segurança tenham os olhos abertos para mudanças e anomalias *todas* as vezes. Hoje em dia, os invasores se tornaram muito hábeis em capturar credenciais por meio de phishing usando aplicações SaaS e lançando outros ataques orientados para nuvem, tornando mais fácil para eles escaparem das defesas da web legadas. Quando o acesso é concedido a um usuário, o trabalho da segurança está apenas começando!

Examinando o comportamento

Um contexto valioso se expande além das questões básicas (às quais nos referimos na seção anterior), detectando e avaliando padrões de comportamento depois que um usuário tem acesso. O Cloud XD aplica análises sofisticadas em busca de pistas de que uma conta foi comprometida, revelando quando um "usuário autorizado" (ou o que parece ser um) se envolve em atividades fora de seu comportamento normal ou função atribuída. O Cloud XD procura sinais de comportamento suspeito para responder a perguntas como:

- Este usuário está fazendo coisas que normalmente não faz, como mover dados?
- O usuário está acessando aplicações ou conteúdo diferentes do normal?
- Quantos dados o usuário está enviando ou baixando, e essa atividade ou quantidade de dados é incomum?
- O usuário está interagindo com o dispositivo de maneira atípica?

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

LEMBRETE

As pessoas podem parecer imprevisíveis, mas suas rotinas e padrões de trabalho são reconhecíveis. O NG SWG desenvolve um perfil de usuário ao longo do tempo e usa esse perfil para detectar ações fora da norma, como movimentação incomum de dados, tentativas de uso indevido de credenciais e muitas outras anomalias.

Explorando o rico contexto externo

Essa abordagem geral, orientada para o contexto, torna a segurança inteligente em relação à nuvem – muito inteligente. Você sabe mais não apenas sobre o contexto interno – o usuário, dispositivo, rede e aplicações que estão todos "dentro" da rede da empresa – mas também sobre o que está fora da rede da empresa. A Netskope possibilita que uma arquitetura SASE compreenda melhor tudo o que faz a nuvem funcionar, como interfaces de programação de aplicações (APIs), que são como as aplicações se comunicam entre si, e JavaScript Object Notation (JSON), que permite que os dados tenham uma estrutura flexível. Os serviços adicionais fornecem informações contextuais sobre sites específicos, serviços de nuvem e repositórios de dados para pintar um quadro completo do ambiente de nuvem no qual o usuário está trabalhando.

Em conjunto, esse contexto torna os serviços de segurança mais eficazes. Como os serviços de segurança agora sabem mais, eles podem agir de forma mais inteligente. Os serviços podem ser controlados por políticas que definem exatamente o que é permitido e o que não é – até detalhes muito específicos e contexto em constante mudança.

Vendo como os serviços são maiores do que a soma de suas partes

No passado, os appliances de segurança frequentemente funcionavam separadamente uns dos outros, realizando suas tarefas individuais em sequência e isoladamente. Em contraste, a arquitetura possibilitada pela Netskope e necessária para um modelo SASE eficaz significa que os serviços podem ajudar uns aos outros conforme necessário, tornando toda a arquitetura mais inteligente. Os serviços de prevenção de perda de dados (DLP) podem trabalhar em conjunto com os serviços de análise de comportamento de usuário e entidade (UEBA) para aplicar níveis extras de proteção de dados quando um usuário exibe um comportamento que indica risco. Por exemplo, o reconhecimento óptico de caracteres (OCR), um serviço DLP avançado, pode ser usado para detectar o que está contido em um documento que um usuário está enviando e, em seguida, determinar se o documento é seguro para compartilhamento. Uma abordagem em equipe sempre vence!

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

O perfil do usuário informa ainda mais o processo, permitindo, por exemplo, que seu diretor financeiro (CFO) compartilhe informações com o contador da empresa, mas evita que um gerente de linha de negócios com acesso compartilhe um subconjunto das mesmas informações com um amigo corretor da bolsa.

Vendo como a segurança funciona quando os usuários são o perímetro

Antes do SASE, a segurança do usuário significava basicamente uma coisa: saber quem é a pessoa. Depois de identificar o usuário, o acesso era concedido além do perímetro para o chamado *castelo* (os dados, aplicações e serviços que o indivíduo estava autorizado a usar). Além disso, a pessoa pode ter tido permissões e restrições específicas que ditam com que coisas ela estava autorizada a trabalhar, sem um entendimento granular mais profundo e certamente sem proteção para comportamentos errantes dentro desses engajamentos permitidos.

ATENÇÃO

SASE ainda começa com o gerenciamento de identidades e acessos – os processos usuais de nome de usuário, senha e autenticação multifator que todos encontramos diariamente em nossas vidas digitais. Mas em uma arquitetura SASE, isso é apenas o começo da verificação da identidade de um usuário. Seus serviços de segurança agora têm um perfil de usuário avançado, detalhado e continuamente atualizado, no qual podem confiar. Todas as outras "coisas" – incluindo o dispositivo que estão usando, a hora do dia, onde estão localizados, as aplicações que estão usando e a velocidade com que digitam – fornecem muito mais informações para confirmar que o usuário é quem diz ser. Mesmo se as credenciais básicas de um usuário forem comprometidas, seus serviços de segurança SASE ainda estão trabalhando para proteger sua empresa e seus dados. (Na arquitetura da Netskope, essa inteligência também é agregada em uma pontuação de risco do usuário. Mais sobre isso no capítulo 4.)

Uma ideia amplamente endossada nos círculos de segurança é o *zero trust:* quando usuários ou dispositivos tentam trabalhar com aplicações e dados nos seus sistemas, presume-se que eles não são confiáveis – de forma alguma – até que possam provar que são quem dizem ser. Mesmo assim, o usuário fica confinado apenas aos recursos definidos para os quais acabou de ser aprovado. Se ele tentar fazer outra coisa, ele deve ser verificado novamente.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

Os princípios de confiança zero podem ser aplicados de forma mais poderosa nas arquiteturas SASE e são outra chave para a implementação adequada de SASE. É a ideia de que, com todo o tráfego de rede, independentemente de você reconhecer o usuário, o dispositivo e assim por diante, você sempre assume que o usuário pode acabar fazendo algo errado.

A confiança zero e uma de suas implementações mais conhecidas, o zero trust network access (ZTNA), não são novidades nos círculos de segurança corporativa, mas a arquitetura SASE expande o escopo de como os princípios de confiança zero podem ser aplicados. Antes da confiança zero, depois que um usuário era autorizado a entrar nos serviços do data center, ele podia estar ainda mais limitado a um conjunto específico de atividades permitidas; dentro desses limites, ele ficava essencialmente livre para fazer o que quisesse.

SASE torna os princípios de zero trust mais fortes e mais flexíveis, até permissivos, para todos os usuários globalmente. (***Lembra-se:*** seus usuários agora são o perímetro! E estão mais para "perímetros", se formos honestos.) A arquitetura SASE aplica o contexto que os usuários têm em todo o tráfego para decisões mais informadas e granulares sobre o que os usuários podem e devem ter permissão para fazer. Em nenhum momento a arquitetura SASE assume que o tráfego de um usuário seja *sempre* bom. Mesmo que seu funcionário conhecido esteja usando uma aplicação SaaS que você deseja que ele use e esteja trabalhando com um conjunto de dados que faz sentido para sua função de trabalho, você simplesmente não assume que o que ele está fazendo com essas duas coisas seja correto.

LEMBRETE

Se você não consegue ver o que está acontecendo dentro de seu tráfego – as interações e transações dentro das conexões que foram permitidas – sua segurança é fraca. Movendo a proteção para *perto* dos usuários, onde quer que estejam acessando dados e distribuindo serviços para esses pontos de acesso de borda, sua segurança pode ver dentro do fluxo de tráfego sem forçar os usuários a voltarem ao seu data center. As pessoas podem trabalhar de qualquer lugar e a política de segurança pode ser aplicada em qualquer lugar.

Reconhecendo Que a Proteção Avançada Contra Ameaças é Melhor na Nuvem

A proteção avançada contra ameaças (ATP) é outra atividade de segurança existente cujo escopo e eficácia aumentam drasticamente em um projeto SASE devidamente implementado. Até recentemente, a ATP se

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

referia apenas a abordagens adotadas para proteger os usuários contra ameaças de entrada, geralmente na forma de arquivos maliciosos.

Mas para ser eficaz em fluxos de trabalho na nuvem, a ATP também deve se concentrar nas ameaças baseadas na nuvem, que incluem não apenas arquivos maliciosos, mas também aplicações e sistemas que podem representar perigos. Na nuvem, você tem novos ângulos de ataque a considerar, incluindo:

- Endpoints ou bordas, como notebooks, tablets, telefones e sensores e dispositivos da Internet das Coisas (IoT), fornecendo informações do mundo externo para seus sistemas internos usando uma conexão em nuvem
- A nuvem, incluindo aplicações SaaS e sites – bons, ruins e todas as variações entre eles, como serviços legítimos cooptados por malfeitores
- Usuários, principalmente a avaliação e verificação das pessoas que atuam em nome da sua empresa

A ATP eficaz na nuvem requer uma abordagem proativa. Ela deve evitar que as ameaças sejam iniciadas quando possível e detectar as ameaças que se manifestam o mais rápido possível. (A Netskope implanta ainda mais serviços de análise de inteligência artificial [IA]/aprendizado de máquina [ML] para ampliar a capacidade de reconhecer problemas.)

O NG SWG está na vanguarda para ajudar a superar esse desafio em grande escala com o Netskope Cloud Threat Exchange, que alimenta seus serviços SASE com um fluxo contínuo de inteligência de ameaças atualizada desenvolvida por *todos* os fornecedores que contribuem para sua plataforma SASE. Além da inteligência derivada do NG SWG, isso inclui a experiência específica de gerenciamento de identidades, proteção de endpoint, informações de segurança, gerenciamento de eventos e outros serviços integrados.

DICA

A variedade de vetores de ameaças possíveis na nuvem é assustadora. Nenhuma organização consegue acompanhar o ritmo sozinha, então uma arquitetura SASE eficaz é o resultado do trabalho em equipe de seus provedores de serviços de segurança.

Evoluindo o proxy para a nuvem

Quando você estava se defendendo apenas contra ameaças básicas da web, sua infraestrutura de segurança provavelmente apresentava um appliance usado para bloquear o acesso de usuários a sites nocivos e para

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

impedir que baixassem malware e outras coisas maliciosas da web. Chamado principalmente de *SWG* e vários outros nomes, como web *proxy* ou *filtragem de conteúdo*, esses sistemas verificam ativamente os URLs solicitados pelos usuários, ficam de olho no que está acontecendo quando as pessoas usam aplicações de comunicação e observam o tráfego de entrada em busca de malwares e vírus conhecidos.

Claro, você ainda precisa dessa funcionalidade, então o NG SWG (consulte o capítulo 2) fornece esses serviços de proxy básicos. Mas, graças ao seu conjunto mais profundo de serviços de inspeção e acesso a amplos recursos de contexto, o NG SWG se posiciona muito mais fortemente contra as ameaças mais recentes possibilitadas pela nuvem. Por exemplo, embora o NG SWG ainda impeça o download de malware, ele também analisa e monitora o tráfego quando alguém está usando Dropbox, Google Workspace, Microsoft Office 365 e qualquer outro SaaS ou serviço baseado em nuvem. Isso torna possível proteger o ambiente de trabalho do usuário, mesmo quando ele está totalmente na nuvem e não está sendo baixado para um sistema corporativo local.

Quando você acerta todas essas coisas, seus usuários ficam mais seguros e capacitados para serem eficazes em seus trabalhos. Seu pessoal está protegido e a organização se beneficia quando seus funcionários são livres para serem produtivos sem comprometer ativos valiosos ou entrar em conflito com questões de conformidade e governança.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

NESTE CAPÍTULO

- **Mudando o jogo da segurança, definindo políticas de alto nível**
- **Usando os superpoderes do NG SWG para controlar os dados onde quer que eles sejam acessados**
- **Superando o desafio de aplicações e serviços em nuvem não gerenciados**
- **Observando a inspeção de passagem única em ação**
- **Compreendendo porque a zero trust é essencial para uma proteção de dados eficaz**

Capítulo 4
Protegendo Dados e Aplicações

No passado, proteção significava manter tudo com segurança dentro do perímetro do seu data center. Hoje, dados e aplicações estão fora da fortaleza do seu data center, eles estão na nuvem. É hora de deixar alguns conceitos desatualizados de proteção de dados permanentemente para trás.

Este capítulo examina como a proteção de dados deve evoluir para ser bem-sucedida e como a tecnologia SASE da Netskope ajuda a garantir que os dados confidenciais de sua organização não sejam mal utilizados, nem fiquem vulneráveis.

Vencendo a Complexidade com o Poder das Políticas

No passado, as equipes de segurança eram limitadas não apenas por sua habilidade, mas também por seu alcance. Suas defesas primárias eram pilhas de appliances de segurança distintos – firewalls, proxies (SWGs), cloud access security brokers (CASBs) e assim por diante. Ambientes

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

de segurança separados e appliances especializados são inerentemente limitados. Pior, depois de enfrentar o microgerenciamento necessário para dizer a cada uma dessas caixas especializadas como fazer seu trabalho, esses sistemas não têm visibilidade, alcance ou poder para proteger adequadamente a nuvem ou trabalhar juntos para prevenir e responder a ameaças. A única opção é bloquear o acesso (veja a figura 4-1), mesmo quando essa política não faz sentido porque o contexto do usuário está disponível.

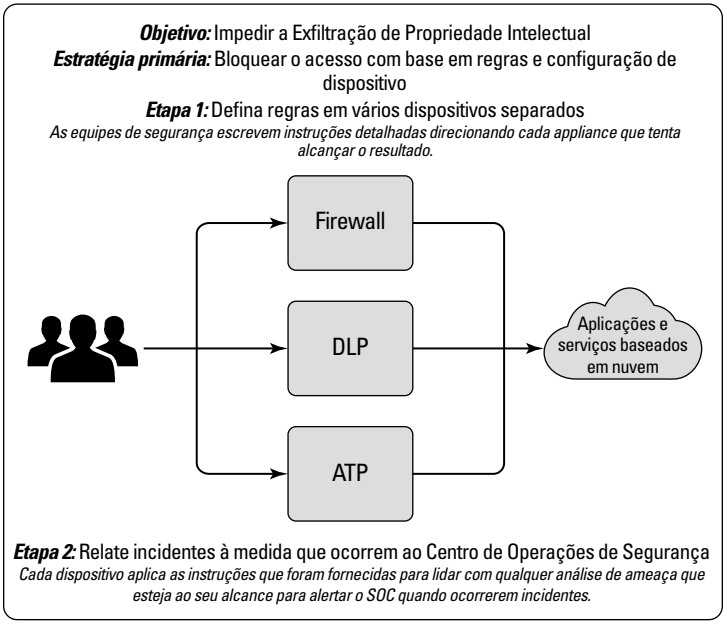

FIGURA 4-1: bloqueando o acesso independentemente do contexto.

A Netskope corrige o problema substituindo aquela bagunça desconexa (veja a figura 4-2). Isso permite que sua equipe de segurança estabeleça políticas abrangentes em nível macro – um conjunto consistente de instruções que descrevem o resultado que você deseja. O next generation SWG (NG SWG) ajuda a transformar essas instruções em ação, coordenando e direcionando os serviços de segurança para alcançar os resultados desejados.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

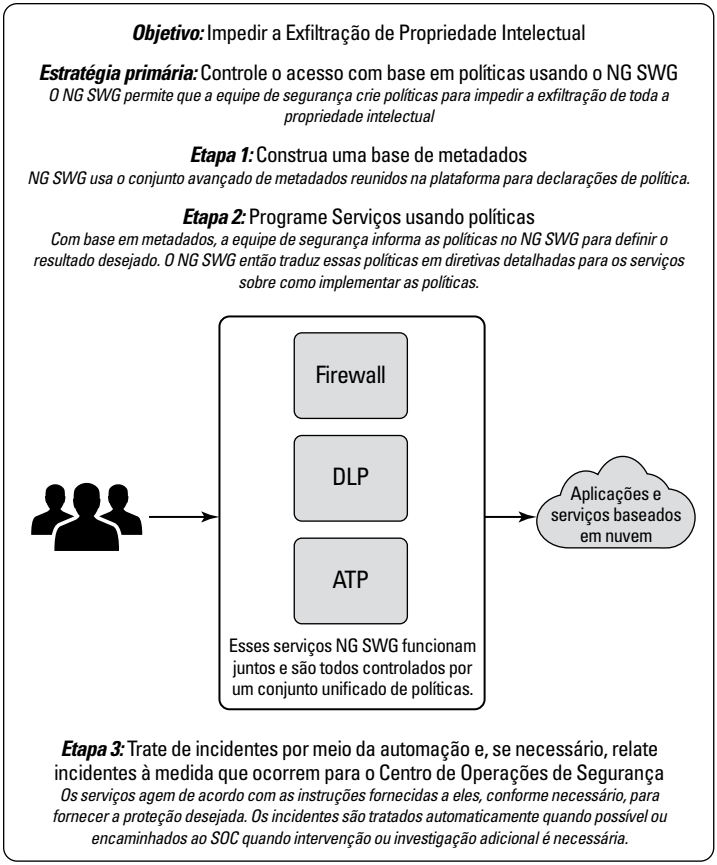

FIGURA 4-2: políticas mais amplas direcionam os serviços de segurança para alcançar os resultados desejados.

Ao contrário de uma abordagem rudimentar de bloquear ou permitir, os controles de política específicos que consideram o contexto e as nuances resultam em menos dispositivos e regras para gerenciar e permitem mais envolvimento do usuário com aplicações e serviços que aumentam a produtividade. Essa abordagem simplifica a vida de sua equipe de segurança. Menos dispositivos para controlar e menos regras para escrever significam menos potencial para erros. Manter e modificar este sistema conforme as necessidades mudam é mais fácil. Mesmo quando os sistemas subjacentes são atualizados e aprimorados, as políticas permanecem as mesmas. Os serviços podem evoluir rapidamente para lidar com novas ameaças porque as mudanças não interrompem a estrutura de segurança.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

Protegendo Dados

Na era anterior à secure access service edge (SASE), os sistemas de prevenção à perda de dados (DLP) rastreavam os dados conforme eles saíam da rede corporativa para evitar que fossem usados ou compartilhados de maneiras não autorizadas e para atender aos requisitos de conformidade. Agora, os dados da empresa vivem cada vez mais fora da empresa, entre serviços e aplicações em nuvem; eles também se movem dentro e entre aplicações em nuvem, às vezes sem nunca tocar no endpoint.

A Netskope observa o tráfego da web e a atividade na nuvem para proteger todos esses dados. O NG SWG lembra o que aprende para aprimorar os serviços de segurança continuamente. Controles especializados fornecem consciência independentemente de qual serviço de nuvem gerenciado ou não gerenciado é usado e se os usuários estão em seus escritórios ou remotamente. O NG SWG reconhece o que os usuários fazem em cada serviço e o que acontece entre os serviços (por exemplo, se um funcionário faz download de dados confidenciais em um serviço gerenciado e, em seguida, tenta enviar esses dados para uma conta pessoal do Gmail).

O NG SWG implementa suas políticas de segurança automaticamente para proteger os dados. Quando você define uma política para proibir o compartilhamento de informações confidenciais, o NG SWG usa seu serviço DLP e classificadores de imagem para notar se um usuário captura uma captura de tela de um slide confidencial do Microsoft PowerPoint ou imagem de um whiteboard com texto confidencial e impede que o usuário envie a captura de tela por e-mail ou para drives compartilhados pessoais ou não gerenciados ou compartilhe os dados em um formulário na web.

LEMBRETE

A inteligência artificial (IA) e o aprendizado de máquina (ML) aumentam a proteção de dados. O NG SWG da Netskope usa IA e ML como poder de fogo extra para detectar detalhes contextuais diferenciados com maior precisão. Essas tecnologias permitem recursos especializados, incluindo:

- **Detecção de padrões e imagens:** usando algoritmos que ajudam a categorizar as informações para fornecer uma classificação dinâmica de risco da página da web ou detectar documentos maliciosos e imagens de informações confidenciais
- **Detecção de anomalias:** reconhecendo ocorrências em dados ou comportamento que são raros, incomuns ou estão fora do lugar

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

Classificadores especializados de IA/ML fazem coisas como determinar quais tipos de imagens estão sendo movidos para reconhecer um conteúdo confidencial, como passaportes, imagens de whiteboards, carteiras de motorista e capturas de tela. Outros classificadores analisam os tipos de documentos para detectar o código-fonte, currículos e outras fontes de dados protegidos. Esse recurso é um poderoso aprimoramento da precisão e eficiência da segurança de dados, importante para proteger o volume de dados que está sendo criado hoje.

Protegendo Aplicações

A organização de hoje depende de várias categorias de aplicações, incluindo aplicações gerenciadas, aplicações não gerenciadas (o que é conhecido como *shadow IT*), serviços de nuvem pública e aplicações personalizadas hospedadas na nuvem pública.

As equipes de segurança já foram capazes de proteger as aplicações contra ameaças externas apenas mantendo os firewalls atualizados. Posteriormente, os firewalls de aplicações da web adicionaram mais proteção. Mas essa proteção foi limitada a aplicações da web executadas dentro do data center.

Quando as aplicações em nuvem chegaram pela primeira vez, os fornecedores de aplicações em nuvem foram solicitados a fornecer interfaces de programação de aplicações (APIs) de gerenciamento que permitissem aos departamentos de TI visibilidade sobre o que os usuários estavam fazendo com as aplicações e lhes proporcionassem um pouco de controle. Essas aplicações, como Salesforce, ServiceNow e Workday, ficaram conhecidas como *aplicações gerenciadas* ou *aprovadas* (veja o capítulo 2)

A Netskope forneceu uma das primeiras ferramentas usadas para esse gerenciamento com seu CASB, que utiliza as APIs fornecidas pelo Google, Microsoft, Salesforce e outras empresas para dar acesso a qualquer recurso de monitoramento e controle que esses desenvolvedores de aplicações incluíram.

ATENÇÃO

O problema para as equipes de segurança é que muitas aplicações valiosas não têm APIs de gerenciamento publicadas. Às vezes, essas aplicações não gerenciadas podem ser avaliadas pela equipe de TI quanto à confiabilidade, segurança e proteção. Mas, como discutimos nos capítulos anteriores, os funcionários costumam usar qualquer aplicação que desejem – resultando nessa shadow IT não autorizada e não monitorada.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

Com o NG SWG, no entanto – e ao contrário do proxy tradicional – a funcionalidade do CASB se expande dramaticamente. Recursos de inspeção profunda distribuídos em toda a Netskope Security Cloud monitoram o Hypertext Transfer Protocol/Secure (HTTP/S) e o tráfego de API de *todas* as aplicações baseadas na web e na nuvem que seus funcionários usam. Isso inclui suas aplicações e serviços gerenciados e não gerenciados anteriormente invisíveis para o CASB. A shadow IT é trazida para a luz!

A Netskope pode descobrir dezenas de milhares de aplicações e serviços em nuvem, atribuindo uma classificação de risco a cada um. Essa classificação de risco é baseada no Cloud Confidence Index da Netskope, uma medida objetiva da prontidão de um serviço em nuvem derivada dos recursos da Netskope e uma variedade de serviços de inteligência de ameaças do setor. O NG SWG usa essa classificação para informar os usuários e equipes de segurança e para orientar a aplicação de suas políticas de segurança. Quando um usuário está conectado aos serviços de nuvem da sua organização, como o Microsoft Office 365, sua atividade é monitorada para que ele não possa baixar dados nessa instância e enviá-los a uma aplicação de nuvem arriscada e não gerenciada.

Vendo a Netskope em Ação

O capítulo 2 descreve a abordagem de inspeção de passagem única do NG SWG da Netskope. Aqui está uma visão mais aprofundada de como o NG SWG aplica essa abordagem para proteger dados e aplicações:

- **Estágio 1:** O NG SWG identifica várias instâncias de aplicações e serviços em nuvem para diferenciar instâncias pessoais, de terceiros e corporativas de aplicações de e-mail e/ou produtividade. O NG SWG usa o sistema de classificação Netskope Cloud Confidence Index para bloquear o acesso a sites maliciosos, aplicações de software como serviço (SaaS) arriscados e serviços em nuvem inseguros. Ele também atua ativamente para impedir que malware e outras ameaças sofisticadas da web se espalhem.
- **Estágio 2:** Usando metadados sobre a identidade, localização, dispositivo e rede do usuário, o NG SWG ajusta o nível de acesso para cada sessão com base nesse contexto. Por exemplo, se o NG SWG determinar que um funcionário totalmente autenticado está usando um tablet pessoal em um ponto de acesso Wi-Fi público, ele pode ser impedido de acessar uma aplicação crítica em nuvem gerenciada.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

- **Estágio 3:** O NG SWG impõe controle sobre as atividades específicas dos usuários para reduzir o risco de vazamento e exposição de dados. Regras sobre upload e download de documentos, compartilhamento de capturas de tela, preenchimento de formulários da web e criação, postagem e publicação em serviços como mídias sociais são aplicadas em cada aplicação e instância.
- **Estágio 4:** O NG SWG monitora continuamente todas as atividades permitidas pelas etapas anteriores, observando anomalias e ameaças. Ele reconhece dados confidenciais em movimento e reage rapidamente com base na confidencialidade dos dados, tipo de ação e outros parâmetros relevantes. Classificadores de imagem aprimorados por ML e técnicas de detecção de padrões entram em ação. O NG SWG pode bloquear certas ações específicas, acionar um alerta, consultar o usuário sobre seus objetivos, solicitar autenticação step-up ou dados de quarentena para inspeção adicional por equipes de segurança. O NG SWG oferece um contexto muito detalhado, portanto, falsos positivos são raros.

O NG SWG implementa amplamente os princípios orientadores do modelo SASE implementado de maneira adequada, de forma que os dados e aplicações sejam protegidos, onde quer que estejam e onde ou como forem acessados.

A Importância dos Princípios de Zero Trust para a Proteção de Dados

A aplicação dos princípios de zero trust é um dos desenvolvimentos mais importantes para a segurança na última década (veja o capítulo 3), e nenhuma discussão honesta sobre a proteção de dados está completa sem isso. A ideia é que nenhum usuário que acesse os dados seja inerentemente confiável e que o acesso às aplicações e dados seja o mínimo possível. Implementações de confiança zero, como zero trust network access (ZTNA), são bem conhecidas nos círculos de segurança e rede. Mas o que significa confiança zero para proteção de dados?

LEMBRETE

Como outras estruturas pré-nuvem, o DLP foi fundado na ideia de que tudo que é importante está dentro de um data center, protegido por um perímetro de rede. Antigamente, a função da proteção de dados era evitar que os dados vazassem de maneiras não autorizadas e impedir que indivíduos não autorizados entrassem no perímetro para acessar esses dados.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

Essa abordagem não funciona na era da nuvem moderna. Alguns dados cruciais estão no data center – atrás do perímetro tradicional – mas pelo menos a mesma quantidade (e cada vez mais) de dados está em aplicações SaaS e em aplicações hospedadas na nuvem pública. As organizações devem repensar a proteção de dados em resposta à forma como os usuários trabalham atualmente, a fim de proteger uma superfície de ataque muito mais ampla e dinâmica. Você precisa de uma maneira de conceder aos usuários acesso apenas aos dados de que precisam, no momento em que precisam, e nada mais.

Em 2021, a Netskope descreveu pela primeira vez o termo zero trust data protection como uma abordagem de segurança que fornece acesso contínuo em tempo real e controle de políticas com base no risco e no contexto. O contexto ajuda a entender o que está acontecendo entre usuários e aplicações e informa como você permite e evita o acesso aos dados com base em um entendimento profundo de quem é o usuário, o que ele está tentando fazer e por quê. Isso é o que permite que as equipes de segurança definam e apliquem controles condicionais com base na confidencialidade dos dados, risco da aplicação, risco de comportamento do usuário e outros fatores – e fazer tudo isso em tempo real. O resultado é uma segurança mais eficaz, graças ao gerenciamento contínuo de riscos.

Uma abordagem de gerenciamento de risco contínuo é a única maneira eficaz de gerenciar o risco dinamicamente em uma combinação de aplicações de terceiros quando você tem uma força de trabalho majoritariamente remota que precisa de acesso permanente a aplicações e dados em nuvem para se manter produtiva (consulte o capítulo 2).

LEMBRETE

A proteção de dados de confiança zero não é apenas uma nova maneira de pensar sobre DLP ou para criar outra ideia de marketing especulativo que se vincula à popularidade do termo *zero trust*. A proteção de dados de confiança zero está no cerne do melhor SASE da categoria, que é levar a segurança e a rede para a era do acesso de qualquer lugar da nuvem e garantir que os dados sejam protegidos em todos os lugares. Uma abordagem unificada e abrangente para SASE e a proteção de dados de confiança zero separam os verdadeiros provedores de tecnologia SASE dos impostores.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

NESTE CAPÍTULO

- **Desenvolvendo um entendimento completo da postura de segurança em nuvem da sua organização**
- **Melhorando as avaliações de risco ao ver a atividade fora do seu data center**
- **Ganhando controle sobre quem está movendo quais dados e para onde**
- **Capacitando e protegendo totalmente sua força de trabalho remota em escala**
- **Refatorando seu data center para trabalhar com segurança com a nuvem**

Capítulo 5
Dez Etapas (ou menos) para se Chegar ao SASE

Este capítulo fornece uma abordagem passo a passo para a implementação de secure access service edge (SASE), desde o conhecimento do seu ponto de partida e para onde você está indo até a otimização e tudo entre eles.

Este capítulo fornece uma visão geral de como obter sucesso implantando o SASE em uma série de sete etapas. Em cada fase, você fará grandes avanços para aumentar significativamente a postura de segurança de sua organização, gerenciando riscos e fornecendo a seus funcionários e clientes a experiência de que precisam.

Etapa 1: Determine Para Onde Você Está Indo

Ao realizar um novo projeto, a necessidade de entregar resultados quantificáveis hoje (ou pelo menos muito rapidamente!) é um desafio significativo enfrentado por um diretor de informações (CIO), diretor de segurança da informação (CISO) ou qualquer pessoa com alto nível

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

de responsabilidade pela rede corporativa e pela segurança. Ao contrário dos projetos de TI típicos em que longos ciclos de desenvolvimento podem ser tolerados, a segurança deve demonstrar valor imediatamente e entregar ganhos rápidos. A vulnerabilidade é assustadora.

SASE aborda essa vulnerabilidade usando uma arquitetura que reflete a forma como a segurança deve ser fornecida *agora* e a convergência crescente (e favorável) de segurança e rede. Mas o verdadeiro modelo SASE é um processo evolutivo de longo prazo. Sua organização crescerá e se tornará SASE. A chave para o seu sucesso é entregar uma sucessão de vitórias tangíveis – saltos deliberados à frente – que repetidamente expandem e fortalecem a segurança da sua organização de maneiras comprovadamente significativas.

Mas, para fazer isso, você deve saber de onde está começando e para onde está indo.

Ao abordar o SASE como uma série de investimentos e implementações bem informados, cada um mudando o jogo em seu próprio direito, você pode entregar resultados dramáticos contínuos enquanto conduz sua empresa para longe de uma visão de mundo centrada em um data center paroquial em direção a uma concepção capaz de colher de forma completa e segura os muitos benefícios da nuvem.

Etapa 2: Ganhe Consciência e Visibilidade

O primeiro passo para resolver qualquer problema é admitir que existe um. Este livro explica como a segurança corporativa não acompanhou as necessidades de segurança e acesso de hoje, mas permaneceu enraizada no data center tradicional.

Mais da metade do tráfego de aplicações corporativas e usuários estão trabalhando em redes que a organização não controla – e isso foi antes da pandemia da COVID-19 tornar o trabalho em casa a nova norma (consulte o capítulo 1).

Você e sua organização precisam enfrentar a gravidade e a amplitude do que escapou de seu controle e a realidade de que as coisas fora de seu controle são como sua empresa faz negócios hoje. Implementar NG SWG de maneira básica, mesmo que para apenas um serviço, acenderá as luzes e mostrará o que está acontecendo e o que não está protegido.

DICA

No mínimo, você precisa de visibilidade completa da atividade do usuário na nuvem se quiser ter confiança em qualquer solução que implementar. Você também precisa da participação dos responsáveis pelas decisões da sua organização. Você consegue aceitação quando esses

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

tomadores de decisão entendem que SASE protegerá coisas essenciais que eles valorizam, mas não percebem que estão perigosamente expostas. Milhões, até bilhões, de dólares em valor são derivados do trabalho que está sendo feito "lá fora".

Etapa 3: Coloque Pontos de Inspeção Centrais Entre Usuários e Aplicações

Com o next generation secure web gateway (NG SWG) firmemente em vigor e sua visibilidade em todo o tráfego drasticamente aumentada, uma coisa é certa: você pode não gostar do que verá a seguir.

Seus funcionários estão usando o Microsoft Office 365? Salesforce? Workday? Box? A resposta é quase certamente que sim. Mas quão grande e quão maduro é esse ambiente de nuvem além do seu perímetro de segurança e fora do que você pode ver facilmente? Quanto dos dados da sua organização está circulando por aí, sem verificação?

Pela primeira vez, sua organização estará ciente do quão exposta ao risco está. Você verá o fluxo de dados, alguns dos quais podem ser particularmente confidenciais, entre sites, serviços e aplicações não seguros.

Agora você tem uma imagem verdadeira e provavelmente preocupante de onde sua organização está em relação à sua dependência do ambiente de nuvem. Muitas aplicações e serviços, poucos controles de segurança eficazes. Até agora.

O NG SWG estabelece um ponto de inspeção central de passagem única, semelhante a um funil, para todo o seu tráfego na nuvem e no data center (consulte o capítulo 2). Esse ponto de inspeção central é melhor do que seu antigo perímetro – muito, muito melhor.

LEMBRETE

Quer isso seja o resultado da shadow IT que foi conscientemente ignorada ou de um processo mais deliberado de digitalização comercial, seus sistemas de segurança antigos e obsoletos estiveram cegos aos detalhes. Ao substituir o proxy antigo e appliances semelhantes, você finalmente terá visibilidade completa sobre quem está usando aplicações e serviços de nível não empresarial e quais dados corporativos estão indo parar "lá fora" além do seu controle. Conforme mostrado na tabela 5-1, o NG SWG e seus novos pontos de inspeção na nuvem permitem que você veja o que está acontecendo dentro de todo esse tráfego: web, software como serviço (SaaS) gerenciado, aplicações de shadow IT, serviços de nuvem pública e aplicações personalizadas na nuvem pública.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

TABELA 5-1 Usando Pontos de Inspeção para Monitorar o Tráfego

Abaixo o velho	Viva a Netskope	A Netskope se integra com...
Proxy legado – apenas sim ou não para o tráfego da web.	Inspeção profunda de todo o tráfego: web, SaaS gerenciado, aplicações de shadow IT, serviços de nuvem pública e aplicações personalizadas na nuvem pública.	Solução de single sign-on (SSO)
Appliance de Secure Sockets Layer (SSL).	A descriptografia de SSL/Transport Layer Security (TLS) é realizada na nuvem em escala de nuvem, sem a necessidade de appliances.	
O cloud access security broker (CASB) legado monitora apenas aplicações gerenciadas que fornecem interfaces de programação de aplicações (APIs).	Monitora as aplicações gerenciadas e também as aplicações não gerenciadas que não oferecem APIs; também vê quais dados estão sendo usados com aplicações, serviços e sites.	

Etapa 4: Introduza Princípios Zero Trust para Acesso à Web, Nuvem e Atividades

É aí que você realmente começará a colocar sua tecnologia para funcionar enquanto estabelece a base de seu projeto SASE. Felizmente, os recursos necessários para acertar as coisas são integrados à plataforma Netskope. Você tem tudo de que precisa para restabelecer o controle sobre os dados da sua empresa, não apenas em sua própria rede, mas também, em última instância, em qualquer lugar na nuvem.

Na etapa 3, conforme mostrado na tabela 5-2, você utilizará controles de segurança expandida para aplicar contexto, indo além das funções sim ou não usadas por seus appliances antigos. O NG SWG também realiza inspeções profundas de seu tráfego da web *e* em seu tráfego na nuvem. E agora que você estabeleceu um novo ponto de inspeção, sua funcionalidade foi expandida para exercer um controle preciso sobre a movimentação e o acesso aos dados, para gerenciar riscos de acordo com as políticas que fazem sentido para o seu negócio.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

TABELA 5-2 **Definindo Políticas para Gerenciar Riscos**

Abaixo o velho	Viva a Netskope	A Netskope se integra com...
Prevenção contra perda de dados (DLP) legada – protege apenas o que está no data center.	A DLP inteligente protege todos os dados que estão sendo movidos para qualquer lugar.	Informações de segurança e sistemas de gerenciamento de eventos e sistemas de proteção de endpoint
Análise de comportamento de usuário e entidade (UEBA)	Detecção de anomalias de comportamento expandida e pontuação de risco do usuário.	
Várias soluções de sandbox.	Proteção avançada contra ameaças (ATP), incluindo sandbox e detecção de anomalias baseada em aprendizado de máquina.	

Etapa 5: Estenda o Zero Trust para Proteção de Dados e Acesso Privado

Agora que sua organização está mais inteligente sobre seu tráfego, capaz de ver o que está acontecendo e de aplicar políticas para proteger seus dados, você pode cumprir a promessa de uma força de trabalho majoritariamente remota. Você possibilitará que as pessoas trabalhem em qualquer lugar e fará com que seja uma experiência excelente, fluida e produtiva que é altamente protetora de seus dados, suas aplicações e seus funcionários.

A mudança mais perceptível é se afastar de sua rede privada virtual (VPN) legada – aquela rota de hairpinning longa e ineficiente que forçava todo o tráfego de seus usuários remotos para o data center em seu caminho para a Internet. Usando a Netskope NewEdge, você pode rotear com eficiência esse tráfego para seu destino enquanto aplica suas políticas de segurança para proteger os dados.

LEMBRETE

Zero Trust significa impor a suposição de que qualquer usuário pode estar fazendo coisas ruins o tempo todo e garantir que os dados estejam sempre protegidos, não importa para onde precisem ir. O profundo conhecimento contextual da plataforma Netskope sobre o usuário, dispositivo, rede, comportamento e centenas de outros detalhes é usado para limitar a atividade apenas ao que foi permitido pela política e para garantir que o usuário seja quem diz ser.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

Depois de implementado, sua segurança e rede serão transformadas para atender às necessidades dos funcionários em nuvem e da segurança dos dados (consulte a tabela 5-3).

TABELA 5-3 Segurança e Rede que Atendem às Necessidades da Força de Trabalho Remota

Abaixo o velho	Viva a Netskope	A Netskope se integra com...
VPN legada	Nuvem de segurança para rotear e proteger o tráfego conforme ditado pela política	Provedores de rede de longa distância definida por software (SD-WAN)
	Acesso à rede de confiança zero (ZTNA)	Sistemas de gerenciamento de identidade para gerenciar e verificar as identidades de usuários e grupos
	Proteção de dados de confiança zero	

Etapa 6: Refatore Controles Internos do Data Center para Gerenciamento de Risco Retroalimentado

LEMBRETE

O data center é apenas mais um lugar para onde as pessoas e os dados devem ir – não é mais o centro das atenções. Quando você está muito adiantado em sua arquitetura SASE, é hora de reconsiderar o data center.

Talvez algumas aplicações que são muito difíceis de mover ou muito preciosas para perder de vista permaneçam no data center. Para acessar essas aplicações, você pode usar o Netskope Private Access, que elimina a VPN e fornece acesso seguro em todo o mundo.

E quanto a todas as outras caixas e bits que foram substituídos pelos serviços da plataforma da Netskope em uma arquitetura SASE? Esta é a sua oportunidade de reduzir drasticamente a complexidade e o custo de manutenção de sua rede, com aqueles sistemas antigos se depreciando e desaparecendo no passado enquanto você e sua empresa olham para frente.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

A tabela 5-4 indica quais sistemas ou tecnologias mais antigos podem ser substituídos usando a plataforma da Netskope.

TABELA 5-4 Fornecendo Acesso Seguro ao Data Center

Abaixo o velho	Viva a Netskope	A Netskope se integra com...
Firewalls, sistema de prevenção de intrusão (IPS), sistema de nome de domínio (DNS)	Fornece proteção de firewall como um dos muitos serviços	Controles de data center legado para ingresso

A verdadeira arquitetura SASE gera economia contínua de custos operacionais. A tabela 5-5 mostra um exemplo de uma arquitetura SASE bem-sucedida. Sua equipe de finanças estará entre os muitos interessados em lhe agradecer!

TABELA 5-5 Economia em Despesas Operacionais Contínuas

Domain	O que acontece	Economia estimada
Domínio	Permite estratégia multi-cloud Melhora a experiência do usuário Simplifica a aquisição e a adoção Permite aplicações lideradas por unidades de negócios	30% em conexões e infraestrutura 20% em custos futuros com nuvem
Acesso multi-cloud	Remove appliances de VPN Tráfego direto para a rede (direct to net) para aplicações com grande largura de banda Reduz as alterações na rede local virtual (VLAN) e nas políticas de firewall	80% em hardware 50% em alterações de segurança e administração
Substituição de VPN	Gerencia o acesso de terceiros Acesso direto a aplicações publicadas Aplica controles granulares por atividade Remove oportunidades de movimentação lateral	80% em hardware 20% em tempo de suporte

(continua)

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

TABELA 5-5 *(continua)*

Domain	O que acontece	Economia estimada
Parceiros de negócios	Onboarding e integração tornam-se mais eficientes Consolida os custos atuais e futuros de rede e segurança Sincroniza a política	40% em hardware O onboarding é cinco vezes mais eficiente

Etapa 7: Monitore, Avalie e Otimize

O caminho para o modelo SASE levará tempo, mas oferece benefícios enormes e transformadores para suas equipes de segurança e sua organização em cada etapa do caminho. A segurança certamente melhora ao longo da jornada, mas o impacto vai muito além disso. Você rapidamente começará a perceber economias de custo, pois os appliances de segurança legados não precisam mais ser mantidos, atualizados e substituídos. Melhor ainda, ao estar totalmente otimizado para a nuvem, não é necessário comprar appliances de segurança de grande gasto de capital e capacidade excessiva não utilizada.

Mas a maneira como SASE funciona na sua empresa será diferente de outro projeto SASE em outra empresa, embora os princípios por trás de SASE sejam os mesmos. Para manter o modelo SASE vivo e saudável, você deve monitorar como ele está funcionando, avaliar onde melhorias são necessárias e tomar medidas para otimizar sua implementação.

Dedicar um tempo para melhorar continuamente protegerá seus ganhos. É difícil exagerar os benefícios que o NG SWG, como parte de uma abordagem de plataforma, traz para a segurança corporativa. Onde antes sua equipe de segurança estava sobrecarregada, tentando entender e correlacionar o que uma dúzia ou mais de aplicações de segurança complexas e independentes estavam tentando dizer a eles no calor do momento, eles agora terão uma plataforma automatizada unificada trabalhando em tempo real. Todos os serviços de segurança entregarão uma mensagem compartilhada e coerente, resultando em menos erros e possibilitando uma ação decisiva – e imediata. Cada pessoa em sua equipe será capaz de fazer mais para aumentar ainda mais a segurança e permitir que seu negócio funcione sem problemas.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

Mais importante, entretanto, é que o modelo SASE devidamente arquitetado com NG SWG transformará as operações de negócios e o relacionamento entre funcionários e tecnologia e entre suas equipes de rede e segurança. A shadow IT pode emergir para a luz, permitindo uma verdadeira transformação digital onde as melhores aplicações e ferramentas da categoria podem ser adotadas com rapidez e segurança para economizar combustível e gerar oportunidades. A experiência do usuário será preservada e seus usuários ficarão felizes e produtivos. Isso só é possível quando a segurança pode apoiar com confiança a inovação digital e a ampla adoção de serviços em nuvem e se alinhar com a rede e todas as partes do negócio nas prioridades de transformação digital. Isso é o que você obtém com a verdadeira arquitetura SASE.

Estes materiais são © 2022 John Wiley & Sons, Inc. Qualquer disseminação, distribuição ou uso não autorizado é estritamente proibido.

A Plataforma de Segurança Inteligente para a Era SASE

A Netskope, líder em Secure Access Service Edge (SASE), conecta os usuários com segurança e rapidez diretamente à Internet, a qualquer aplicação e sua infraestrutura a partir de qualquer dispositivo, dentro ou fora da rede. Com CASB, SWG e ZTNA construídos nativamente em uma única plataforma, a Netskope é rápida em qualquer localidade, centrada em dados e cloud-smart, ao mesmo tempo que permite uma boa cidadania digital e oferece um custo total de propriedade menor.

Visite www.netskope.com para obter mais informações.

netskope

Crie uma arquitetura SASE que proteja os dados e gere um valor comercial duradouro

Em um mundo digital que deixou os limites restritivos do data center para as possibilidades abertas da nuvem, uma arquitetura secure access service edge (SASE) é a única arquitetura que faz sentido. Capacite seus usuários, proteja seus dados e expanda seus negócios com uma arquitetura SASE bem projetada que combina cloud access security broker (CASB), next generation secure web gateway (NG SWG) e princípios de confiança Zero Trust como catalisadores para o sucesso.

Conteúdo...

- Saiba mais sobre a evolução dos dados, aplicações, redes e segurança
- Compreenda as funções do CASB, NG SWG e Zero Trust na arquitetura SASE
- Proteja sua força de trabalho remota em grande escala e melhore a experiência geral de seus usuários
- Crie um plano confiável para o futuro de sua segurança e rede

Os líderes da Netskope **Jason Clark** (CSO), **Lamont Orange** (CISO) e **Steve Riley** (Field CTO) são autoridades amplamente reconhecidas em nuvem, segurança e rede, com décadas de experiência em organizações globais, incluindo Ernst & Young, Gartner, Optiv, Riverbed e Websense.

Acesse Dummies.com®
para ver vídeos, fotos passo a passo, artigos how-to ou para fazer compras!

ISBN: 978-1-119-85518-7
Proibida a revenda

para leigos®

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.