Trazido para você por:

netskope

Security Service Edge (SSE)

para leigos

Desenvolva sua TI para o futuro da segurança na nuvem

Forneça CASB, SWG, ZTNA e firewall a partir de uma única plataforma

Entenda o SSE como parte de uma arquitetura SASE e Zero Trust

Edição especial da Netskope

Jason Clark

Steve Riley

Sobre a Netskope

A Netskope, líder em SASE, conecta os usuários com segurança e rapidez diretamente à Internet, à qualquer aplicação e à sua infraestrutura a partir de qualquer dispositivo, dentro ou fora da rede. Com CASB, SWG, firewall como serviço e ZTNA integrados nativamente em uma única plataforma, o Netskope Security Cloud fornece o contexto mais granular, por meio de tecnologia patenteada, para permitir o acesso condicional e o reconhecimento do usuário, ao mesmo tempo em que aplica os princípios Zero Trust em proteção de dados e prevenção contra ameaças em todos os lugares. Ao contrário de outros que o forçam a escolher entre segurança e rede, a nuvem privada de segurança global da Netskope oferece recursos completos de computação na borda.

A Netskope é rápida em qualquer lugar, centrada em dados e inteligente na nuvem, ao mesmo tempo em que permite uma boa cidadania digital e fornece um custo total de propriedade mais baixo. Obtenha mais informações em www.netskope.com.

Gostaríamos de agradecer a várias pessoas que tornaram este livro possível:

Da Netskope: Amanda Anderson, Lauren Baker, Chad Berndtson, Jeff Brainard, Tim Chiu, Tom Clare, Catie Halliday, Maxwell Havey, Scott Hogrefe, Kathy Jacobsen, Sasi Murthy, Shamla Naidoo, Lauren Polito, Zoe Revis, James Robinson, James Yokota, Svetlana Rubin

Da Evolved Media: David Penick, 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.

Security Service Edge (SSE)

para leigos®

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

Security Service Edge (SSE)

Edição especial da Netskope

Jason Clark e Steve Riley

para leigos®

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

Security Service Edge (SSE) 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: EMBORA A EDITORA E OS AUTORES TENHAM USADO SEUS MELHORES ESFORÇOS NA PREPARAÇÃO DESTE TRABALHO, ELES NÃO FAZEM REPRESENTAÇÕES OU GARANTIAS COM RELAÇÃO À PRECISÃO OU À INTEGRIDADE DO CONTEÚDO DESTE TRABALHO E ESPECIFICAMENTE ISENTAM-SE DE TODAS AS GARANTIAS, INCLUINDO, SEM LIMITAÇÃO, QUAISQUER GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO OU DE ADEQUAÇÃO PARA UM PROPÓSITO ESPECÍFICO. NENHUMA GARANTIA PODE SER CRIADA OU ESTENDIDA POR REPRESENTANTES DE VENDAS, MATERIAIS DE VENDAS ESCRITOS OU DECLARAÇÕES PROMOCIONAIS PARA ESTE TRABALHO. O FATO DE UMA ORGANIZAÇÃO, SITE OU PRODUTO SER MENCIONADO NESTE TRABALHO COMO UMA CITAÇÃO E/OU POSSÍVEL FONTE DE INFORMAÇÕES ADICIONAIS NÃO SIGNIFICA QUE O EDITOR E OS AUTORES ENDOSSAM AS INFORMAÇÕES OU OS SERVIÇOS QUE A ORGANIZAÇÃO, O SITE OU O PRODUTO PODE FORNECER OU RECOMENDAÇÕES QUE PODE FAZER. ESTA OBRA É VENDIDA COM O ENTENDIMENTO DE QUE A EDITORA NÃO PRESTA SERVIÇOS PROFISSIONAIS. AS ORIENTAÇÕES E AS ESTRATÉGIAS CONTIDAS NO PRESENTE DOCUMENTO PODERÃO NÃO SER ADEQUADAS PARA A SUA SITUAÇÃO. CONSULTE UM ESPECIALISTA QUANDO APROPRIADO. ALÉM DISSO, OS LEITORES DEVEM ESTAR CIENTES DE QUE OS SITES LISTADOS NESTA OBRA PODERÃO SER ALTERADOS OU RETIRADOS NO PERÍODO EM QUE O LIVRO FOI ESCRITO E QUANDO FOR LIDO. NEM A EDITORA NEM OS AUTORES SERÃO RESPONSÁVEIS POR QUAISQUER PERDAS DE LUCRO OU QUAISQUER OUTROS DANOS COMERCIAIS, INCLUINDO, ENTRE OUTROS, DANOS ESPECIAIS, INCIDENTAIS, CONSEQUENCIAIS OU OUTROS TIPOS DE DANO.

Para obter informações gerais sobre nossos outros produtos e serviços, ou sobre como criar um livro personalizado *Para Leigos* para sua empresa ou organização, entre em contato com nosso Departamento de Desenvolvimento Comercial 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 *Para Leigos* para produtos ou serviços, entre em contato pelo e-mail BrandedRights&Licenses@Wiley.com.

ISBN 978-1-119-89665-4 (pbk); ISBN 978-1-119-89666-1 (ebk)

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

Editor gerente sênior: Rev Mengle

Representante de desenvolvimento de negócios: Jeremith Coward

Responsável pela produção: Tamilmani Varadharaj

Ajuda Especial: Nicole Sholly

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

Índice

INTRODUÇÃO 1

Sobre Este Livro 1
Suposições Tolas 2
Ícones Usados Neste Livro 2
Além do Livro 2

CAPÍTULO 1: Como o Contexto e a Integração Aceleram a Transformação da Segurança 3

Para Onde a Segurança Aponta 4
Forçando a Transformação da Segurança 6
Criando o Nirvana da Segurança 7

CAPÍTULO 2: Como a Nuvem Quebrou o Modelo de Segurança Tradicional 9

Lembrando Quando o Firewall Dominava a Segurança 10
Compreendendo Como a Nuvem Beneficia as Empresas 11
Produtos Individuais Ajudam em Determinadas Situações, Mas Não Resolvem os Grandes Problemas 12
Integrar a Segurança É Imperativo 13
A Segurança Deve Acompanhar os Dados 14
SSE: Orientando as Necessidades de Segurança da Jornada Rumo ao SASE 15
Precisamos de Segurança para Amanhã, Não para Ontem 16

CAPÍTULO 3: Security Service Edge: Um Plano para o Futuro da Segurança em Nuvem 17

Explorando Por Que Precisamos do SSE 18
Descobrindo Como o SSE Concilia os Serviços de Segurança 20
Análise em Etapas de Passagem Única 20
Desenvolvido por Serviços Compartilhados 21
SSE: Principais Atrativos 22
Recursos SSE: Em Breve para Sua Equipe de Segurança 24
Classificação Aprimorada para Oferecer Suporte ao DLP 24
Gerenciamento de Postura de Segurança para Nuvem e SaaS 25
Reconhecimento e Neutralização de Ameaças 25
Gerenciamento da Experiência Digital 26
A Rede Também Deve Evoluir 26
A Recompensa da Segurança do SSE 28

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

CAPÍTULO 4: **Usando Zero Trust para Dar Vida ao SASE** 29
Do Zero Trust à Confiança Adaptativa Contínua 30
Quatro Etapas Simples para o SSE 33
1ªEtapa: Migrar trabalhadores móveis para recuperar a visibilidade 33
2ª Etapa: Migrar os funcionários restantes e aplicar a classificação de dados em toda a empresa 34
3ª Etapa: Implementar confiança adaptativa contínua e serviços ampliados 35
4ª Etapa: Gerencie o risco proativamente com análise e pontuação dinâmicas 35
Transformando a Rede e o Resto da Segurança 36
Benefícios Comerciais do SSE 37

CAPÍTULO 5: **Dez (ou Mais) Dicas do que Fazer e do que Não Fazer na Jornada Rumo ao SSE** 39
Faça dos Dados o Foco 40
Adote a Integração 40
Lembre-se de que os Malfeitores Também Estão na Nuvem 40
Reconheça que a Segurança É uma Parte Fundamental da Estratégia de Negócios 41
Não Pense em Silos 41
Não Transfira Regras Antigas 42
Não Odeie o Data Center 42
Não Tenha Medo de Mudanças 42

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

Introdução

A transição geral dos negócios para a nuvem está acontecendo muito mais rápido do que muitos especialistas previam. Essa velocidade deixou a maioria das empresas dependentes de plataformas de segurança criadas para um mundo passado e dominado por data centers on-premises. A pandemia da COVID-19 acelerou e complicou ainda mais a situação, pressionando os CISOs responsáveis por proteger uma equipe de trabalho em casa que pode não retornar totalmente ao escritório.

A boa notícia é que o Secure Access Service Edge (SASE), uma estrutura de arquitetura de segurança, aponta o caminho para uma solução em nuvem que fornece a proteção que toda empresa precisa, onde quer que seus funcionários estejam localizados. Melhor ainda é a notícia de que o Security Service Edge (SSE), o conjunto fundamental de serviços de segurança no SASE, fornece os recursos necessários para implementar serviços de segurança para proteger trabalhadores remotos, tecnologia em nuvem e aplicações e infraestrutura on-premises existentes.

SASE é uma estrutura. SSE é um conjunto de serviços que você pode adquirir hoje. Este livro explica o SSE e explora sua base, a qual é construída a partir de ideias inovadoras como Zero Trust, segurança adaptável baseada em contexto e novas abordagens para design de rede. O livro mostra como os serviços familiares são interligados dentro do SSE, juntamente com tecnologias novas e avançadas que podem aumentar drasticamente a segurança.

Sobre Este Livro

É hora de reformular o cenário de segurança moderno. Aprender sobre o SSE ajudará a equipe de segurança e de negócios a se preparar para as etapas necessárias para refazer a segurança corporativa – atualmente um gargalo – como um amplificador e facilitador da transformação digital. O livro prepara o cenário com explicações sobre SASE e SSE e, em seguida, oferece um roteiro de como você pode dar vida à essa nova segurança. O uso da nuvem exige que todas as empresas transformem sua segurança. Este livro aconselha sobre como se preparar.

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 ou à segurança. Você sabe que o modelo de segurança tradicional que todos nós usamos já está no limite. Você também está ciente de que a nuvem é tanto um impulsionador de produtividade quanto um lugar perigoso onde as credenciais e os dados de indivíduos e empresas estão sob ataque. Por último, você tem interesse em amenizar esse desafio para sua empresa, funcionários, acionistas, clientes e parceiros de negócios usando o poder representado pelo SASE e pelo SSE.

Ícones Usados Neste Livro

Usamos ícones em todo o livro para destacar informações importantes.

DICA

O ícone Dica oferece atalhos e outras informações que podem facilitar sua vida.

LEMBRAR

O ícone Lembrar sinaliza fatos que são especialmente importantes.

ATENÇÃO

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

Além do Livro

Para obter mais informações sobre as soluções Netskope, visite `www.netskope.com`. Para um aprofundamento contínuo sobre Security Service Edge (SSE), `visite www.netskope.com/security-defined/security-service-edge-sse`.

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

NESTE CAPÍTULO

- **Explorando o futuro da segurança**
- **Compreendendo como a transformação digital afeta a segurança**
- **Descobrindo como criar o nirvana da segurança que todos desejamos**

Capítulo 1
Como o Contexto e a Integração Aceleram a Transformação da Segurança

As organizações mudam para aplicações em nuvem para usufruir de benefícios comerciais concretos como velocidade, eficiência e a percepção que a nuvem oferece. Para proteger de fato dados, pessoas e aplicações na nuvem, a segurança não pode mais consistir em decisões binárias simples de aceitação/rejeição que se aplicavam nos dias em que a rede era suprema e a maioria dos funcionários trabalhava no mesmo lugar. A segurança deve ser mais inteligente, usando contexto detalhado para criar a proteção certa para sua organização, independentemente de onde seus funcionários estejam localizados. A segurança deve acompanhar os dados aonde quer que eles vão, e deve ser fácil de aplicar para não retardar os negócios.

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

Para Onde a Segurança Aponta

Agora é um momento significativo para estar imerso na segurança. O poder e a qualidade da tecnologia de segurança cibernética estão fazendo avanços surpreendentes. Nunca os profissionais de segurança tiveram que lidar com tantas mudanças tão rapidamente e eles nunca tiveram uma oportunidade como a atual de transformar a segurança em um facilitador estratégico de negócios. Dados, aplicações e trabalhadores migraram para a nuvem. A segurança deve segui-los.

As empresas que adotarem uma postura de segurança em nuvem para permitir a transformação digital inovarão com mais rapidez e segurança do que as empresas cuja postura de segurança está arraigada em torno das ideias de ontem. Prevemos uma nova era em que os profissionais de segurança finalmente saltarão à frente dos invasores e oferecerão suporte às empresas à medida que a transformação digital em nuvem ganhar impulso.

Os esforços para forçar os sistemas de segurança legados para a nuvem não estão dando certo. Sob uma estrutura descrita como Secure Access Service Edge (SASE), a segurança está se transformando para atender ao local de trabalho híbrido baseado em nuvem.

ATENÇÃO

Os melhores produtos e serviços de segurança do passado não terão sucesso na nuvem. Nem a readaptação ou a renomeação da tecnologia de segurança antiga como "habilitada para nuvem".

Em vez disso, os fornecedores de tecnologia de segurança estão oferecendo novos produtos e serviços nativos da nuvem para fornecer proteção quando os dados são armazenados e as aplicações são executados em uma infraestrutura que as próprias empresas não controlam. A nova tecnologia de segurança deve proteger não apenas o *acesso* aos dados, mas também o *uso* desses dados.

É útil olhar para a segurança pronta para nuvem através de quatro ideias fundamentais:

- **SASE** é a estrutura para implementar uma infraestrutura convergente em nuvem para funções de rede e de segurança. SASE reúne conceitos como Zero Trust (confiança zero), SD-WAN e Security Service Edge (SSE) para nos guiar a uma postura de segurança e rede que protege e governa a nuvem e o novo ambiente de trabalho em qualquer lugar. Os analistas reconhecem que essa nova arquitetura oferece segurança abrangente para um mundo centrado na nuvem. (Consulte Desenvolvendo *uma Arquitetura SASE para Leigos* da Netskope para obter uma introdução completa.)

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

- **SSE** é a forma como todos os serviços de segurança necessários para SASE – que antes eram aplicações, produtos ou serviços separados, geralmente de fornecedores diferentes – se reúnem em uma forma unificada e integrada que oferece maior capacidade e eficiência e reduz a complexidade e o custo. SSE representa recursos de segurança profundamente integrados que estão cientes uns dos outros, funcionam bem juntos e são fornecidos por um único fornecedor. A Netskope define ainda um conjunto de recursos estendidos que chamamos de SSE adequado (consulte o capítulo 3).
- **Contexto** determina como os recursos de segurança integrados de SSE são aplicados como o mecanismo de controle para manter dados, aplicações e pessoas seguros o tempo todo. Contexto – uma compreensão profunda de *quem* a pessoa é, *o que* ela está tentando fazer, e *por que* ela está tentando fazer isso (além de quando, por que e como) – também possibilita a aplicação de políticas de segurança adaptativa para reduzir o risco em tempo real. Anteriormente, "permitir" ou "bloquear" eram as únicas opções. Agora, o contexto rico oferece suporte a níveis de controle de acesso, como "permitir, com condições", para fornecer uma segurança verdadeira sem prejudicar a produtividade. A qualidade e a amplitude do contexto são um diferenciador essencial entre os fornecedores de segurança.
- Os princípios de Zero Trust (confiança zero) diferenciam políticas verdadeiramente adaptativas de autenticação condicional simples com base na familiaridade. O objetivo não é apenas fornecer o acesso e a autorização de que cada pessoa necessita para realizar determinada tarefa, de acordo com o nível de confiança derivado de uma avaliação em tempo real da identidade do funcionário e do método de acesso. O acesso adaptativo requer informações sobre o que acontece *depois* do login – sinais ambientais que variam ao longo do tempo, comportamento histórico e atual, e as características dos próprios dados. Na Netskope, vemos a confiança zero como o ponto de partida (nenhuma confiança no início de cada interação) e almejamos o objetivo de *confiança adaptativa contínua*, onde a quantidade de confiança é compatível com o nível de confiança determinado e sinais ambientais.

Este livro explica como esses conceitos se fundem em SSE efetivamente implementado para criar um novo nirvana de segurança (consulte o Capítulo 3). As empresas finalmente desfrutarão da segurança em nuvem com tudo o que é necessário para proteger um mundo de dados e aplicações centrado na nuvem, acessado por funcionários que

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

estão distribuídos (e continuarão assim) e muitas vezes longe de um escritório central.

Forçando a Transformação da Segurança

Explosões em várias áreas da transformação digital estão remodelando o mundo dos negócios. A transformação da segurança é vital para alcançar e manter o sucesso dos esforços de transformação digital.

LEMBRAR

Tecnologias como a nuvem, Internet das Coisas (IoT), aprendizado de máquina/inteligência artificial (ML/IA) e análises melhoram substancialmente os resultados dos negócios. Se a segurança não puder acompanhar, esse progresso estará em risco.

- **A explosão de dados:** até 2025, a IDC prevê que haverá 175 zetabytes (ZB) de dados em todo o mundo (até 25x desde 2010). Como você pode ver nas manchetes, os invasores estão roubando dados de empresas para fins nefastos – para vendê-los, modificá-los de forma maliciosa ou para obter resgate. O Netskope Threat Labs descobriu que a nuvem é um *playground* de invasores, com 68% do malware entregue pela nuvem em 2021 (em comparação com menos da metade em 2020). A explosão de dados acessados da nuvem gera mais alvos para os invasores e mais desafios para os defensores.
- **A explosão da nuvem:** as empresas estão adotando infraestrutura e aplicações em nuvem para ganhar velocidade, flexibilidade e agilidade. De acordo com o Netskope Threat Labs, uma empresa média assina mais de 800 aplicações de software como serviço (SaaS) distintas. Espantosos 97 por cento deles são chamados de "shadow IT", o que significa que não são gerenciados (e em muitos casos, não são visíveis para) a equipe de TI interna. Além disso, as configurações de segurança padrão de muitas aplicações em nuvem estão totalmente abertas – outro motivo pelo qual os invasores consideram a nuvem um alvo particularmente interessante.
- **A explosão dos dispositivos:** as estimativas variam amplamente quanto ao volume de dispositivos conectados à Internet no horizonte, de 25 bilhões em 2025 a surpreendentes 75 bilhões, talvez em 2030. Mais dispositivos e mais conectividade criam um estado de tecnologia maior – e uma superfície de ataque maior. No entanto, explosões de dispositivos muitas vezes levam a uma inovação acelerada.

LEMBRAR

A transformação da segurança consiste em criar uma nova maneira de lidar com todas essas explosões para que a empresa possa fazer o que for necessário para ter sucesso.

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

As empresas que não conseguem se envolver na transformação da segurança em nuvem enfrentam riscos crescentes. O cenário de segurança atual tornou-se muito complexo, custando às empresas grandes quantias em despesas de capital (CapEx), despesas operacionais (OpEx) e horas de trabalho, mesmo quando sua eficácia declina. Os fornecedores devem, portanto, reconstruir funções em sistemas que colaboram entre si.

Criando o Nirvana da Segurança

As empresas que estão planejando seu futuro de segurança devem imaginar como será o nirvana da segurança, tanto em traços gerais quanto em detalhes. Conselhos práticos – não é marketing nem exagero (há alguma diferença?!) – devem orientar suas decisões.

Em linhas gerais, é assim que essa transição pode ocorrer:

1. **Transforme a rede.**

   A rede deve mover dados da maneira mais eficiente possível entre todos os pontos, incluindo serviços em nuvem e o data center, sem trocar desempenho e experiência do trabalhador por segurança. O tráfego é roteado por meio de uma rede construída para suportar SSE que consiste em pontos de presença (PoPs) globalmente distribuídos. Os funcionários no escritório, em casa ou na cafeteria recebem segurança e desempenho de alto nível, e os dados da empresa permanecem protegidos.

2. **Consolide os serviços de segurança.**

   Um pacote de um fornecedor único que oferece um SSE abrangente substitui a colcha de retalhos de dispositivos de segurança legados. Os recursos mesclados simplificam o gerenciamento e a administração, garantem a aplicação uniforme das políticas e otimizam o processamento do tráfego.

3. **Estenda o uso de SSE e implemente serviços de segurança avançados.**

   Com SSE em vigor, as equipes de segurança podem introduzir funções poderosas, como isolamento remoto do navegador (Remote Browser Isolation, RBI), gerenciamento de postura de segurança na nuvem (cloud security posture management, CSPM) e gerenciamento de postura de segurança SaaS (SaaS security posture management, SSPM). Recursos avançados, como prevenção contra perda de dados (data loss prevention, DLP) e proteção avançada contra ameaças (advanced threat protection,

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

ATP), têm melhor desempenho do que em modelos antigos, prejudicados por integração mínima e visibilidade restrita.

4. **Proteja os dados na nuvem e nos dispositivos da empresa.**

   O mesmo fornecedor de SSE também deve fornecer um firewall como serviço (firewall as a service, FWaaS) para proteger aplicações em nuvem, dispositivos de propriedade da empresa e repositórios de dados.

5. **Trate o data center como apenas mais um destino.**

   O data center corporativo tradicional, antes o único destino pelo qual todo o tráfego era devolvido, torna-se mais um destino para o qual o SSE direciona o tráfego. Eliminar o hairpinning diminui o custo, reduz a complexidade e aumenta o desempenho.

6. **Aplique os princípios de confiança zero para alcançar um estado de confiança adaptativa contínua.**

   Como o SSE monitora constantemente o tráfego depois que o acesso é concedido, os profissionais de segurança podem conduzir uma análise contextual completa da sessão, tomar decisões informados por inteligência de risco de terceiros, detectar mudanças nos perfis de risco e neutralizar ações perigosas. Notificações podem treinar os funcionários para melhorar seus hábitos de segurança.

7. **Melhore o gerenciamento de riscos em toda a empresa com maior visibilidade.**

   A capacidade de ver, orientar e controlar a atividade de todos na empresa melhora drasticamente a percepção e a detecção de riscos. A equipe de segurança pode se concentrar em áreas de alto risco e implantar mais rapidamente políticas aprimoradas no SSE para reduzir o risco. Os líderes de segurança podem se engajar em discussões sobre riscos e estratégias de negócios que os elevam a posições vitais na mesa dos tomadores de decisão.

Uma transformação de segurança não é um empreendimento pequeno. O Capítulo 4 mostra como os princípios de confiança zero permitem uma mudança incremental para a implementação completa de segurança em nuvem. O Capítulo 5 destaca erros comuns e princípios de sucesso, e descreve uma jornada representativa que muitas empresas seguirão se abordarem SSE, confiança zero e, em última análise, SASE da maneira certa.

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

NESTE CAPÍTULO

- **Revendo a história do firewall**
- **Investigando por que a nuvem veio para ficar**
- **Aceitando as limitações de produtos individuais**
- **Explorando como a segurança deve ser integrada e acompanhar os dados**
- **Reconhecendo o papel que o SSE desempenha nas necessidades de segurança**

Capítulo 2
Como a Nuvem Quebrou o Modelo de Segurança Tradicional

Há uma década, poucos líderes previam a rapidez com que todas as formas de nuvem se estabeleceriam nos negócios. As empresas agora assinam, em média, mais de 800 aplicações de software como serviço (SaaS), de acordo com o Netskope Threat Labs.

A computação em nuvem e de borda está enviando cada vez mais cargas de trabalho de negócios para fora do data center. As iniciativas de trabalho em qualquer lugar, aceleradas pela pandemia da COVID-19, inspiraram mais pessoas, dispositivos, aplicações, serviços e dados a escapar dos limites tradicionais do data center corporativo. A nuvem agora é fundamental para a produtividade empresarial. Mas, à medida que novos riscos se materializam, a nuvem também está nos forçando a repensar a segurança.

Considere como os pais protegem seus filhos enquanto são bebês e crianças pequenas. Dentro de suas casas, eles adicionam proteção para crianças em escadas, tomadas elétricas, armários e assentos sanitários infantis. Os pais protegem o perímetro interior com um alarme que

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

alerta sempre que uma porta se abre. Eles protegem o perímetro externo com uma cerca no quintal. Depois que mandam seus filhos para a creche, para a escola e mais tarde (nossa, como o tempo passa!) para a faculdade, o objetivo de proteger seus filhos continua o mesmo, mas o papel dos pais mudou.

Da mesma forma, os objetivos de proteger a nuvem significam reconhecer que o objetivo da segurança — proteger dados, aplicações e indivíduos — não mudou. O que mudou é que os dados, as aplicações e os indivíduos saíram de casa, reduzindo o papel do firewall e deixando-o bem para trás. Enquanto isso, as ameaças que mais crescem estão na nuvem, não no seu data center. O resultado: as táticas de segurança devem mudar.

Lembrando Quando o Firewall Dominava a Segurança

Antigamente, o firewall era seu ponto de controle de segurança central mais importante e provavelmente era o item de linha mais caro no seu orçamento de segurança. A maioria das empresas projetava suas arquiteturas de segurança de rede em torno do data center, cercado por um perímetro bem definido. Ser seguro significava proteger sua rede.

No mundo pré-nuvem, essa abordagem fazia sentido. Afinal, o data center era um único local onde uma empresa armazenava seus valiosos ativos digitais. Como uma casa bem protegida por alarmes hoje, uma empresa erguia um perímetro (na maior parte) impenetrável em torno do seu data center. Um portão poderoso construído com dispositivos de segurança de acesso restrito. Assim como um pai com alarmes em portas e janelas, você tinha um controle substancial da segurança de sua empresa naquele mundo pré-nuvem.

Os funcionários percorriam uma rede exclusiva e privada que os conectava às áreas que necessitavam para realizar seu trabalho. Aqueles que estavam em filiais distantes ou trabalhando remotamente viajavam até a rede privada, digitavam o código do alarme e obtinham permissão para acessar não apenas as aplicações e os dados internos, mas também todos os destinos conectados externos. Fazer o backhaul do tráfego de trabalhadores remotos por meio desse data center centralizado dentro do perímetro e, em seguida, para fora aumentava o custo e a complexidade e paralisava o desempenho.

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

A segurança de firewall antiga era uma simples questão de permitir ou de negar acesso. Depois de receber acesso, a presença e as boas intenções de um indivíduo eram tidas como certas. Como parte da segurança em perímetro, as empresas adotavam a segurança projetada para impedir ameaças individuais ou categorias de ameaças à medida que surgiam. Quando uma ameaça surgia, comprava-se um outro equipamento. No modelo on-premises, uma empresa poderia ter uma linha de dez caixas de segurança conectadas por um fio.

Cada caixa realizava sua própria inspeção. Ela aplicava seu próprio "Ei, quero detectar malwares... quero comparar assinaturas e bloquear invasões... quero filtrar e-mails, ou eu quero escanear dados confidenciais... quero me proteger contra ataques de resolução de nomes... quero fornecer bloqueio de porta e de protocolo com listas de controle de acesso." Cada função fazia seu trabalho e em seguida encaminhava pacotes para a próxima função na linha, o que aumentava a latência e a complexidade.

A nuvem mudou todas as antigas pressuposições.

Compreendendo Como a Nuvem Beneficia as Empresas

A computação em nuvem oferece flexibilidade e valor comercial tão profundos que, à esta altura, não há como voltar atrás. (E você pode ignorar reivindicações tempestuosas de "repatriação" para data centers corporativos. Exceto para cenários raros e específicos, esse simplesmente não é o caminho.) A nuvem é atraente para CEOs, CFOs, CIOs e empresas em geral porque a maior parte da infraestrutura é comoditizada e pronta para o uso. A nuvem impede o gasto de muito tempo e dinheiro investindo na sua própria infraestrutura. Você assina uma nuvem, ativa-a, personaliza-a para atender aos seus requisitos comerciais exclusivos e a usa. À medida que as empresas buscam acelerar a geração de receita e se tornar mais lucrativas, a migração para a nuvem é parte da resposta.

A nuvem também é atraente para seus funcionários ocupados. Eles são atraídos pelas aplicações SaaS amplamente disponíveis que oferecem plataformas modernas e às vezes agradáveis para colaborar, se comunicar, tratar de finanças, fechar vendas e administrar relacionamentos com clientes. Essas aplicações de terceiros na nuvem parecem melhores, mais rápidas e mais eficazes do que qualquer coisa oferecida por aplicações corporativas antigas e desajeitadas nos limites rígidos do data center de uma organização.

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

ATENÇÃO

Mas aí está o problema – e o perigo: a maioria dessas aplicações em nuvem não é aprovada, muito menos controlada, pelo departamento de TI corporativa — e dificilmente é segura. Você ainda tem o dever de proteção, mas não tem mais o tipo de controle ao qual estava acostumado. Adotar a nuvem é como mandar seus filhos para a escola ou mesmo para a faculdade — você não consegue vê-los nem sabe o que estão fazendo.

Na era da nuvem, o firewall não é mais seu controle de segurança mais importante porque ele não protege sua empresa de forma abrangente contra ameaças na nuvem. Sem segurança adequada para proteger e abranger nossos processos digitais, funcionários, clientes e (hm hm) ativos; neste novo cenário aberto, os esforços de aceleração digital serão arriscados. Na era da nuvem, o trabalho da segurança é permitir o valor comercial criado pela nuvem, gerenciando o risco que também é criado pela nuvem.

Produtos Individuais Ajudam em Determinadas Situações, Mas Não Resolvem os Grandes Problemas

À medida que os funcionários saíram dos escritórios e os dados e as aplicações migraram para a nuvem, as ferramentas de segurança legadas instaladas no data center ficaram cegas para as atividades que aconteciam além do perímetro. As aplicações SaaS exigiram que dados originados *dentro* das muralhas fossem úteis. No entanto, as próprias aplicações estavam do *lado de fora* das muralhas, tornando os dados que migraram para elas descontrolados e desprotegidos pela segurança corporativa.

A mudança era necessária se as empresas quisessem tirar vantagem segura das aplicações em nuvem. As empresas configuraram novos produtos individuais com foco restrito em suas redes privadas e na nuvem para resolver os problemas de segurança e as fraquezas mais urgentes relacionadas ao uso da nuvem. Essas ferramentas incluíam:

- **Agentes de segurança de acesso à nuvem (Cloud Access Security Brokers, CASBs)**: Os CASBs ajudam a controlar e a proteger os dados corporativos armazenados no computador de outra pessoa, o que é uma maneira honesta de conceituar a nuvem.
- **Secure Web Gateways, SWGs(SWGs):** Os SWGs protegem funcionários e organizações contra ameaças na Web — ou seja, as páginas que um funcionário visita quando está on-line e navegando em sites públicos.

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

- **Acesso Zero Trust à rede (Zero Trust Network Access, ZTNA):** Os produtos ZTNA simultaneamente protegem do público as aplicações privadas de uma empresa e disponibilizam as aplicações para um conjunto de funcionários conhecidos.

Essas ferramentas representaram uma geração inicial de segurança na nuvem. Mas essa geração inicial também carecia de algo fundamental: integração.

Integrar a Segurança É Imperativo

Os produtos de segurança em nuvem da geração anterior geralmente vinham de provedores diferentes e, como resultado, não funcionavam juntos. Cada um oferecia seu próprio console e exigia a configuração de políticas duplicadas e sobrepostas (pense em DLP aqui). Cada um podia exigir um agente exclusivo, criando desafios de implantação e de direcionamento de tráfego. E cada um exigia negociações contratuais e acordos de compra separados.

Imagine se seus sentidos de audição, olfato, paladar, visão e tato estivessem conectados a diferentes cérebros. Sem integração, ao ver um incêndio, sentir o cheiro de um incêndio ou ouvir um incêndio, você não sabe o que fazer porque seu cérebro que vê, seu cérebro que cheira e seu cérebro que ouve não estão compartilhando informações. Eles não estão correlacionando as contribuições de todos os seus sentidos.

Nessa infraestrutura de segurança, há muitos sistemas diferentes, cada um com seu próprio cérebro especializado em seu domínio específico. Por exemplo, o CASB é um cérebro focado principalmente em "tenho um funcionário tentando acessar uma aplicação SaaS".

LEMBRAR

Assim como seu cérebro adquire informações de todos os seus sentidos para tomar decisões sobre como se comportar no mundo, seus serviços de segurança devem ser totalmente integrados para tomar decisões eficazes que apoiem sua estratégia na nuvem. O SSE é o cérebro que integra diferentes categorias de segurança. Em vez de operar separadamente em sequência, o SSE permite que todos esses "sentidos" de segurança sejam ativados em paralelo. O resultado: segurança mais rápida e mais eficiente. Além disso, o SSE é muito mais fácil de adquirir, pois todos os recursos (CASB, SWG, ZTNA e relacionados) são adquiridos juntos em uma única transação.

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

A Segurança Deve Acompanhar os Dados

Como explicamos no Capítulo 1, o Secure Access Service Edge (SASE) descreve uma visão na qual o perímetro empresarial tradicional não existe mais. Em vez disso, todo o portfólio de funções de rede e recursos de segurança são migrados para a nuvem, onde ficam imediatamente adjacentes aos funcionários, aos dados armazenados na nuvem e às aplicações SaaS.

O SASE fornece uma maneira de ajustar nossa perspectiva em um mundo que prioriza a nuvem e funciona em qualquer lugar, onde a antiga noção de perímetro físico desapareceu. Neste novo mundo, a segurança deve ir muito além dos limites do data center. A segurança agora deve acompanhar o ativo mais importante de uma empresa — seus dados — com um nível de reconhecimento contextual suficiente para proteger esses dados em qualquer lugar em que residam e de qualquer modo que sejam acessados.

Para fornecer segurança que aborda a nuvem, novas premissas e recursos de segurança devem estar em vigor. A segurança deve:

- Acompanhar os dados.
- Basear-se em um contexto rico.
- Adaptar-se às características específicas do contexto de um funcionário.

A outra consideração importante que um modelo SASE resolve é o equilíbrio entre a segurança e o desempenho da rede. Não podemos trocar um pelo outro – precisamos dos dois. As pessoas são mais produtivas quando sua experiência com a tecnologia é fácil e tranquila. Quando as ferramentas de segurança diminuem a velocidade das redes, o desempenho diminui e a produtividade sofre. Ou ainda pior, os funcionários tentam ignorar completamente os controles de segurança, o que cria um tremendo risco e exposição.

O passo crucial para alcançar esse equilíbrio é que uma empresa migre seus recursos essenciais de rede e de segurança para a nuvem, eliminando dispositivos em perímetro e (prepare-se para enfrentar a resistência) todos os produtos legados.

Esta abordagem fornecerá acesso seguro e confiável a serviços da Web, aplicações e dados, com princípios Zero Trust aplicados para obter confiança adaptativa contínua durante todas as interações.

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

SSE: Orientando as Necessidades de Segurança da Jornada Rumo ao SASE

O SASE e o SSE são a forma como a segurança migra para a nuvem e se torna mais eficaz do que qualquer coisa que tivemos antes.

O SASE é uma visão geral para a transição de recursos de rede e de segurança em direção à nuvem. O SSE é o cérebro que integra, identifica e executa um conjunto específico de serviços de segurança necessários para alcançar o SASE. O conjunto de serviços integrados torna-se o principal ponto de inspeção onde a inspeção e o controle de segurança consistentes são aplicados a todo o tráfego. O SSE não substitui o firewall — você ainda terá um — mas ele suplanta a posição do firewall como seu recurso central de segurança.

CASB, SWG, ZTNA e outros serviços relacionados certamente possuem seu valor individualmente. A maioria das empresas já implantou um ou dois deles. No entanto, para aproveitar todo o valor da nuvem, esses serviços devem ser integrados e precisam trabalhar juntos.

A Netskope acredita que as funções essenciais do SSE podem ser ampliadas com muitos recursos atualmente ausentes na segurança corporativa, mas cruciais para proteger de maneira confiável os ativos digitais além dos limites do data center. Eles incluem:

- **Classificação:** identifica e rotula informações confidenciais, de preferência quando são criadas, mas também por meio de verificações periódicas de armazenamentos de dados.
- **Prevenção contra perda de dados (Data Loss Prevention, DLP):** monitora e controla ativamente o movimento de informações confidenciais.
- **Reconhecimento e neutralização de ameaças (também conhecida como proteção avançada contra ameaças ou ATP – Advanced Threat Protection):** identifica indicações que um ambiente foi comprometido e executa medidas para reduzir ou eliminar a probabilidade de um ataque futuro.
- **Gerenciamento de postura de segurança na nuvem (Cloud Security Posture Management, CSPM):** avalia a configuração de nuvens de infraestrutura e de plataforma e toma medidas para corrigir configurações incorretas que possam resultar em um comprometimento.
- **Gerenciamento de postura de segurança SaaS (SaaS Security Posture Management, SSPM):** avalia a configuração de aplicações

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

SaaS e elimina configurações incorretas que possam permitir exfiltração, falsificação ou outros tipos de ataque.

- **Gerenciamento de experiência digital (Digital Experience Management, DEM):** analisa os dados coletados para fins de segurança junto com outros sinais de disponibilidade e de desempenho para medir a experiência do funcionário e ajudar a resolver problemas rapidamente.

LEMBRAR

Ao reunir todos esses recursos em um único produto de segurança integrado implantado na nuvem, mais próximo das pessoas, dados e aplicações, o SSE se torna o ponto de inspeção mais importante que protege sua empresa. (Examinaremos o SSE em detalhes no Capítulo 3.)

Precisamos de Segurança para Amanhã, Não para Ontem

Devemos implantar ferramentas que auxiliem a nuvem, o fator-chave na criação de valor e de receita de negócios. Devemos implantar ferramentas que resistam a interrupções causadas por cibercriminosos. E por fim, devemos implantar ferramentas que não impeçam as operações. Imagine esse conceito como enviar um guarda-costas invisível com seu filho para a creche, a escola e a faculdade. Esse guarda-costas portátil é o SSE.

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

NESTE CAPÍTULO

- Entendendo a necessidade do SSE
- Explorando os recursos e os requisitos do SSE
- Avaliando os benefícios do SSE

Capítulo 3
Security Service Edge: Um Plano para o Futuro da Segurança em Nuvem

O Secure Access Service Edge (SASE) muda nossa perspectiva de como a segurança é fornecida em um mundo baseado em nuvem, em que os dados podem ser acessados em qualquer lugar. Quando os funcionários são remotos, quando as aplicações se tornam software como serviço (Software as a Service, SaaS) e quando os dados são migrados para a nuvem, os esforços de segurança cibernética de uma organização também devem ser migrados para a nuvem. Devidamente implementado, o SASE nos mostra que a segurança deve estar o mais próximo possível de onde os dados residem e são acessados. No SASE, a segurança protegerá os interesses de uma organização e fornecerá controles consistentes, independentemente de quão distantes esses interesses estão, sem prejudicar a conectividade da rede e a experiência do usuário.

Parte da obtenção do SASE é a consolidação e integração da segurança — a própria essência do SSE.

O SSE transfere pontos críticos de controle e inspeção para a(s) nuvem(s) onde sua empresa opera. Essa mudança coloca a segurança ao lado de

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

onde os dados, as aplicações e as pessoas operam – e onde está o perigo. Com o SSE, serviços de inspeção e controle para SaaS, Web e dados, além de reconhecimento e neutralização de ameaças sofisticados, funcionam como um sistema único, coerente e interoperável.

DICA

Você não tem um problema de rede. Você tem um problema de segurança na nuvem. A única conversa necessária sobre rede é sobre adotar uma arquitetura que torna o SSE o principal ponto de inspeção na nuvem.

O SSE fornece recursos que transcendem o que os firewalls tradicionais podem fazer. O SSE implementado adequadamente também discerne o contexto – os detalhes de o que, como e por que os dados são acessados – permitindo que ele tome decisões de segurança diferenciadas em tempo real. O SSE conecta todos os seus "sentidos" de segurança em um único cérebro que interpreta os dados, compreende a amplitude dos riscos apresentados e negocia o nível certo de acesso a qualquer momento, em qualquer situação.

Adiante, veremos como o SSE funciona.

Explorando Por Que Precisamos do SSE

A antiga abordagem de segurança era baseada no estabelecimento de um perímetro e na implantação de um firewall para tentar repelir invasores que visavam seu data center corporativo. Mas como nenhuma segurança é inviolável, um invasor que violou o perímetro com sucesso estava livre para se movimentar lateralmente por toda a rede, tornando seus dados e aplicações efetivamente indefesos.

As arquiteturas SASE ainda contam com o gerenciamento de identidade e de acesso para autenticar o funcionário e em plataformas de proteção de terminais para proteger os dispositivos. Mas o SASE eficaz também implementa os princípios Zero Trust que concedem acesso e monitoram a confiança com base em um conjunto abrangente de condições. Na nuvem, o contexto em torno da pessoa torna-se o perímetro.

Zero Trust é uma filosofia baseada em três proposições fundamentais para o SSE e, portanto, para o SASE:

- A confiança implícita presente em projetos legados sobreviveu à sua utilidade. Zero Trust inverte a confiança, ou seja, verifique para ter certeza, depois confie. Toda pessoa ou ação que solicita acesso aos dados deve ter sua identidade e contexto verificados toda vez para chegar a um determinado nível de confiança. Sem exceções.

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

- Forneça apenas acesso mínimo, também conhecido como privilégio mínimo, apropriado para o nível de confiança determinado. O acesso é limitado a um recurso específico e não é transferível para outros recursos.
- O contexto deve ser constantemente reavaliado com base em sinais como, por exemplo, a identidade do funcionário, a identidade do dispositivo, a postura de segurança do dispositivo, a hora do dia, a geolocalização, a função comercial e a confidencialidade dos dados. Cada mudança de sinal deve desencadear uma nova reavaliação. (A Netskope chama isso de *confiança adaptativa contínua*, e abordaremos isso mais profundamente no Capítulo 4.)

O SASE fornece uma estrutura para um programa Zero Trust eficaz, abrangendo totalmente ambientes nos quais pessoas, aplicações e dados estão em qualquer lugar. Mas, conforme discutiremos mais adiante no Capítulo 4, Zero Trust é um conjunto de princípios, não uma arquitetura técnica de como implementar diferentes funções de segurança de forma unificada.

O SSE fornece essa arquitetura técnica. O SSE unifica, integra e coordena muitos serviços de segurança, aprimora os recursos de segurança e fornece alto desempenho para os funcionários e as necessidades dos negócios, de forma integrada e personalizada com base no contexto. Para proporcionar os resultados desejados, o SSE fornece:

- Contexto detalhado, incluindo histórico do funcionário, dispositivo, dados solicitados, aplicação, rede e até mesmo o motivo da solicitação.
- Informações sobre os recursos que a pessoa tem permissão para acessar para atender à solicitação, o que o SSE pode colher dos detalhes de autorização e direitos.
- Detalhe granular que classifica a confidencialidade de diferentes recursos de dados (para evitar perda de dados).
- Orientação e um conjunto detalhado de políticas que descrevem o resultado de segurança desejado com base em várias combinações de pessoas, dados, aplicações e outras informações contextuais.

A dificuldade é que muitos dos resultados de segurança, como DLP e reconhecimento e neutralização de ameaças, exigem que vários componentes de segurança funcionem juntos.

ATENÇÃO

A implementação de cada serviço de forma independente requer a repetição de uma quantidade razoável de trabalho de segurança nos consoles de uma ferramenta após a outra. Isso é complicado e propenso a erros quando uma venda – ou uma vida – está em jogo.

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

O SSE elimina a repetição. Quando implementado corretamente, ele reúne esses serviços e permite que eles compartilhem contexto, direitos, políticas de segurança, inteligência de risco, isolamento de navegador, codificação/descodificação de dados e muito mais. Essa coesão capacita os serviços de segurança a processar transações em uma única passagem para fornecer o acesso adequado rapidamente.

Descobrindo Como o SSE Concilia os Serviços de Segurança

O SSE baseia-se na integração de muitos serviços de segurança suportados por vários recursos relacionados. Há uma maneira certa de construir o SSE... e muitas maneiras erradas.

ATENÇÃO

À medida que o termo SSE ganha popularidade, o marketing enganoso logo se seguirá. O SSE construído incorretamente é facilmente reconhecido pela sua falta de integração. As abordagens que apenas vinculam processos discretos ou atualizam cadeias de dispositivos antigos são evidências de sistemas criados a partir de componentes separados, construídos em estilos legados pré-nuvem e possivelmente adquiridos de vários provedores. Esses sistemas integrados apresentam uma latência significativa, não oferecem os amplos benefícios do SSE e não são etapas significativas na sua jornada geral rumo ao SASE.

O SSE nunca é uma cadeia de dispositivos ou uma sequência de processos discretos em que os dados podem passar por um mecanismo DLP, depois um avaliador de lista de controle de acesso, em seguida um gateway da Web e assim por diante. No entanto, é útil separar as características que descrevem um SSE totalmente integrado.

Análise em Etapas de Passagem Única

LEMBRAR

Em um SSE ideal, os serviços de segurança integrados operam em paralelo. Todas as inspeções ocorrem simultaneamente, em tempo real, independentemente de o tráfego ser da Web, da nuvem ou do seu data center.

Uma passagem única típica fornece uma filtragem de tráfego cada vez mais refinada para proteger os dados e as aplicações. Comece imaginando o tráfego fluindo por um funil.

O SSE adequado diferencia entre aplicações corporativas (por exemplo, Salesforce, Workday), aplicações pessoais (como a conta do Gmail de um indivíduo) e aplicações/serviços de terceiros (como instâncias da empresa no Microsoft Office 365 ou Dropbox). Ele usa esse conhecimento

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

para iniciar as conexões apropriadas necessárias para proteger cada aplicação ou serviço de acordo com a política.

O SSE adequado avalia o contexto, ajustando o acesso com base em, por exemplo, se um médico (consulte o Capítulo 4) está usando um tablet de propriedade do hospital no quarto de um paciente, seu celular no Wi-Fi da cafeteria ou um computador para jogos no quarto do seu filho.

O SSE adequado impõe políticas para evitar que os dados sejam perdidos ou vazem. Os controles podem impedir o download de documentos, capturas de tela, inserção de dados em formulários da Web ou postagens em redes sociais.

O SSE adequado oferece monitoramento contínuo. À medida que o funcionário realiza atividades corriqueiras, o SSE está atento a anomalias. Quando os objetos de dados são confidenciais, o SSE pode diferenciar entre conteúdo confidencial e não confidencial, alterando dinamicamente as permissões de acesso e as atividades permitidas. O SSE pode acionar um alerta, emitir avisos ou consultar o funcionário para obter mais informações para orientar sua atividade com segurança.

Desenvolvido por Serviços Compartilhados

Todas as funções de segurança de alto nível, incluindo DLP, reconhecimento e neutralização de ameaças, gerenciamento de experiência digital (Digital Experience Management, DEM) e outras, podem usar um ou todos os serviços e técnicas que descrevemos aqui para alcançar os resultados de segurança desejados:

- **Contexto compartilhado:** todos os elementos SSE compartilham uma enorme coleção de metadados que identificam a pessoa, o dispositivo e o local. O site, a aplicação ou o serviço de destino é identificado e recebe uma avaliação de risco, e suas atividades são avaliadas. Quaisquer dados solicitados ou criados pelo funcionário e a aplicação são considerados. O contexto rico do SSE inclui uma avaliação do comportamento do funcionário, até mesmo referenciando interações passadas para analisar a atividade atual. Esse ambiente contextual constantemente atualizado informa as medidas tomadas e as políticas aplicadas por todos os elementos do SSE. (No SSE da Netskope, este serviço é chamado de Cloud XD.)
- **Confiança adaptativa contínua:** o acesso a dados e a aplicações não é uma decisão simples e binária. O acesso deve ser flexível com base nas mudanças de requisitos e de contextos. O SSE adequado alinha a quantidade de confiança com o valor dos ativos que

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

estão sendo acessados, orientados pela vasta riqueza de sinais contextuais disponíveis e pelo apetite da organização por risco, conforme ditado pela política.

- **Administração baseada em políticas:** como parte da segurança de passagem única, o SSE adequado apresenta uma estrutura de política detalhada e compartilhada que permite que a organização estabeleça os limites de sua tolerância ao risco e defina claramente os resultados de segurança esperados. Isso representa um afastamento significativo das milhares de regras que normalmente ocupam os firewalls. Os componentes do SSE consultam a estrutura de políticas para controlar atividades e dados em todas as aplicações, categorias de aplicações e serviços da Web.

SSE: Principais Atrativos

Agora que descrevemos os componentes subjacentes do SSE, podemos examinar os recursos que o SSE oferece. Alguns serão coisas familiares que sua organização já implantou de outra forma, portanto, é provável que o SSE os substitua com o passar do tempo.

LEMBRAR

O SSE visa permitir que as pessoas e a sua empresa trabalhem da maneira mais rápida e segura possível. Ao funcionar em todos os lugares, o SSE acaba com os esforços inúteis para melhorar a segurança no seu data center para acompanhar dados, aplicações e pessoas que migraram para a nuvem.

A tabela 3-1 mostra os requisitos mínimos de recursos para que um produto seja descrito como SSE com precisão de acordo com vários analistas em 2021.

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

TABELA 3-1 **Requisitos Mínimos para Recursos SSE**

Recurso	O Que Faz	Como o SSE o Melhora
SWG	Controla o acesso e defende apenas contra ameaças da Web.	Também aborda ameaças e riscos de dados habilitados para a nuvem para instâncias pessoais de aplicações gerenciadas, milhares de aplicações de shadow IT e serviços em nuvem.
CASB	Um ponto de execução de políticas de segurança colocado entre os consumidores de serviços em nuvem e os provedores de serviços em nuvem para impor políticas de segurança corporativas à medida que os recursos em nuvem são acessados. Avalia o comportamento e tem conhecimento da funcionalidade da aplicação SaaS para definir o acesso apropriado para uma determinada pessoa.	Elimina a duplicação de políticas (entre SWG e CASB), simplifica a administração (agente único para SWG, CASB e ZTNA) e fornece visibilidade em todas as faixas de tráfego.
ZTNA	Impõe a premissa de que ninguém é cegamente confiável e autorizado a acessar os ativos da empresa até que seja validado como legítimo e autorizado. Suporta a implementação de acesso de privilégio mínimo, o qual concede seletivamente acesso apenas a recursos que pessoas ou grupos de pessoas requerem, nada além disso.	Melhora o ZTNA, fornecendo capacidade de acesso adaptável. Harmoniza a administração e a decisão de políticas com outros componentes de SSE enquanto ainda mantém a execução de políticas distribuídas.
Isolamento de navegador remoto (Remote Browser Isolation, RBI)	Separa os dispositivos de trabalho do ato de navegação na Internet, hospedando e executando todas as atividades de navegação em um container remoto em nuvem. Essa área restrita protege dados, dispositivos e redes de todos os tipos de ameaças provenientes de sites maliciosos.	Permite que o RBI use a classificação de dados e o contexto de funções. Adiciona isolamento ao conjunto de medidas de política em SWG e CASB.

(continua)

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

TABELA 3-1 *(continua)*

Recurso	O Que Faz	Como o SSE o Melhora
Firewall como serviço (Firewall as a Service, FWaaS)	Segurança de rede para todas as portas e protocolos de saída para acesso seguro e direto à Internet por meio de um agente em dispositivos gerenciados ou via GRE e IPsec para escritórios. Um só mecanismo de política e uma só plataforma de segurança, fornecendo gerenciamento simplificado para funcionários e filiais usando um console.	Permite que as organizações agreguem tráfego de várias fontes — seja de data centers no local, filiais, trabalhadores móveis ou infraestrutura em nuvem. Fornece aplicação consistente e aplicação de segurança de políticas em todos os locais e para todos os funcionários, ao mesmo tempo em que oferece visibilidade e controle completos da rede sem implantar dispositivos físicos.

Recursos SSE: Em Breve para Sua Equipe de Segurança

O SSE desenvolverá maiores recursos à medida que os produtos amadurecerem e as iniciativas focadas em nuvem se proliferarem. A arquitetura SSE adequada abrange muito mais do que a definição de uma referência original, como:

- Classificação aprimorada para suportar DLP
- Gerenciamento de postura de segurança para nuvem e SaaS
- Reconhecimento e neutralização de ameaças
- Gerenciamento da experiência digital

Abordaremos cada um deles nas seções a seguir.

Classificação Aprimorada para Oferecer Suporte ao DLP

DLP é um nome genérico para um recurso destinado a impedir a exfiltração intencional e acidental de dados por uso indevido intencional e

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

não intencional. O DLP detecta o movimento de informações confidenciais, evita que elas se espalhem para locais indesejados, interrompe os funcionários com pop-ups educacionais para interromper a exposição não intencional e incorpora o aprendizado de máquina para avaliar as pontuações de risco do funcionário.

DICA

O SSE melhora o DLP identificando e classificando ativamente os dados, possibilitando rastrear e aplicar regras relacionadas à movimentação de dados confidenciais com mais precisão.

Gerenciamento de Postura de Segurança para Nuvem e SaaS

O gerenciamento de postura de segurança na nuvem (Cloud Security Posture Management, CSPM) e o gerenciamento de postura de segurança SaaS (SaaS Security Posture Management, SSPM) descobrem e corrigem configurações incorretas nas nuvens (a forma mais comum de falha de segurança na nuvem). Utilizando o contexto fornecido pelo SSE, pelos controles habilitados para interface de programação de aplicação (Application Programming Interface, API) e pela avaliação em tempo real de implantações de nuvem pública, o CSPM e o SSPM mitigam o risco analisando a configuração, sugerindo alterações que reduzem ou até eliminam a probabilidade de um possível ataque, e monitorando a conformidade regulatória.

DICA

O CSPM e o SSPM em implementações adequadas de SSE reconhecem as ameaças e tomam medidas ativamente para aumentar a postura de segurança de uma organização.

Por exemplo, algumas implementações de CSPM e SSPM podem identificar a não conformidade quando a política de uma organização requer a criptografia de todos os dados na nuvem por padrão. Esta é uma postura muito forte a ser adotada porque exige controles de acesso que devem concordar que: a identidade de uma pessoa deve estar presente na lista de controle de acesso de um objeto criptografado e na lista de sua chave de criptografia associada. O CSPM e o SSPM reconhecem quando uma pessoa tem acesso a um, mas não ao outro e sinalizam a inconsistência.

Reconhecimento e Neutralização de Ameaças

O reconhecimento e a neutralização de ameaças descobrem evidências de ataques bem-sucedidos e acionam alarmes para que o perigo possa ser contido. A evidência típica inclui atividade de rede incomum, alterações na configuração e exclusão de arquivos de registro. A análise forense determina se uma ameaça ativa está no ambiente. A neutralização de

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

ameaças é um exemplo perfeito de um serviço que se beneficia e contribui com evidências para os recursos compartilhados da arquitetura SSE.

Gerenciamento da Experiência Digital

Um aspecto emergente e poderoso do SSE é sua capacidade de avaliar a experiência do funcionário e o desempenho da aplicação, especialmente porque o limite da rede agora se estende até a nuvem e além. Ao fornecer monitoramento contínuo de todo o tráfego, os clientes se beneficiam de uma visibilidade completa na sua rede e de comportamento de aplicações com informações acessíveis em tempo real com base na atividade humana real para garantir que o SSE funcione sem comprometimentos de desempenho. Quando surgem problemas de dispositivo, rede ou aplicação, o DEM (gerenciamento da experiência digital, Digital Experience Management) pode ajudar a identificar as causas-raiz rapidamente, acelerar a resolução de tíquetes de suporte técnico e fornecer etapas proativas para evitar que pequenos problemas se tornem grandes eventos de impacto nos negócios.

A Rede Também Deve Evoluir

Até este ponto, focamos nos recursos de segurança que o SSE oferece para um mundo que prioriza a nuvem. Mas é necessária mais transformação além do que pensamos como segurança.

LEMBRAR

O acesso à rede deve ser distribuído para permitir que funcionários e organizações extraiam o valor total dos sistemas em nuvem que o SSE está protegendo, conforme mostrado na Figura 3-1.

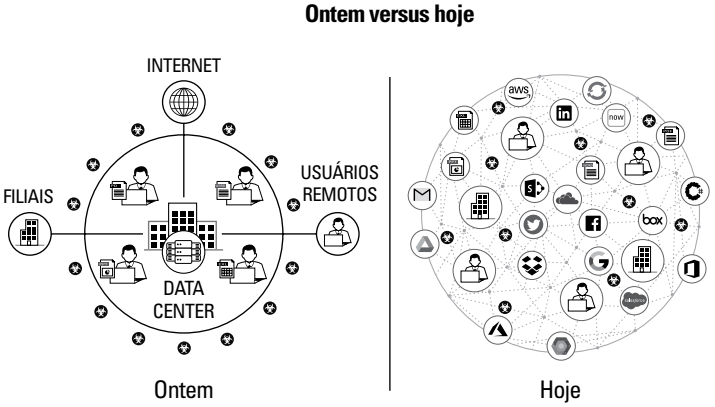

FIGURA 3-1: O antigo modelo de acesso era ineficiente e ineficaz em relação ao novo modelo, o qual permite o acesso em qualquer lugar.

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

No antigo modelo de acesso, os funcionários se conectavam à uma rede protegida por um perímetro bem definido. As filiais mantinham conexões caras de rede privada com o data center. Isso se tornou um obstáculo à medida que as operações de negócios floresciam, primeiro na Web e depois na nuvem. A única opção segura era desviar o tráfego de funcionários através da pilha de segurança do data center antes de interagir com os recursos da nuvem e da Web.

Esta abordagem é ineficiente e ineficaz. Permitir que os funcionários interajam diretamente com os recursos da nuvem melhora muito o desempenho e a produtividade, mas subverte a visibilidade e o controle do data center. Persistir no modelo antigo construindo, mantendo e monitorando redes privadas para alcançar tudo o que a nuvem pode oferecer é complicado, caro e simplesmente não consegue acompanhar o mesmo ritmo em uma era em que a segurança deve ser uma prioridade máxima em todos os níveis de negócios, incluindo a diretoria.

O novo modelo de rede prevê uma arquitetura construída para trabalho remoto, onde as pessoas se conectam de qualquer lugar e interagem com outras pessoas e informações predominantemente na nuvem. Para melhor desempenho e experiência de aplicação, a rede de um provedor de SSE deve:

- Emparelhar-se com inúmeras conexões para os destinos que mais importam
- Consistir em um número suficiente de pontos de presença equipados com recursos computacionais completos e distribuídos estrategicamente para que os funcionários nunca estejam longe

DICA

A maneira de obter conexões rápidas e sem esforço é trabalhar com um provedor cuja rede seja altamente emparelhada com várias conexões diretas para os destinos mais importantes. Quanto mais conexões seu provedor oferecer, melhor será o desempenho, mais forte será sua resiliência e mais satisfeitos ficarão os usuários.

LEMBRAR

Um provedor bem conectado oferece melhor desempenho, resiliência mais forte e experiências agradáveis. A experiência do funcionário importa! A transformação digital é bem-sucedida quando a segurança e a rede se fundem em uma parceria coesa desde o primeiro dia. A segurança que degrada o desempenho da rede — ou que força uma troca perigosa entre segurança e produtividade — não serve.

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

Como todos os aspectos do SASE e do SSE, a transformação da rede é otimizada ao longo do tempo. Seu provedor de segurança em nuvem deve superar a divisão entre a segurança que você tem agora e onde deseja estar no futuro. Ele deve fornecer SSE, proporcionar novas rampas de acesso para sua força de trabalho distribuída e integrar-se perfeitamente à infraestrutura e aos processos de rede existentes.

A Recompensa da Segurança do SSE

Ao adotar uma arquitetura SASE com princípios Zero Trust no seu núcleo e fazer parceria com um provedor de SSE capaz de fornecer serviços de segurança essenciais e distribuídos, uma organização pode esperar benefícios significativos:

- Maior confiança ao conceder acesso a dados e a aplicações fora do data center
- Segurança flexível baseada em informações sobre risco com políticas adaptáveis e controle sobre atividades específicas sob medida para cada aplicação
- A capacidade de estender os princípios Zero Trust além de aplicações privadas para abranger aplicações da Web e SaaS
- Acesso a serviços de segurança adicionais, como RBI e DLP avançado, com base no nível avaliado de risco ou de confiança
- Monitoramento contínuo sobre mudanças no contexto que acionam automaticamente uma reavaliação de confiança e de acesso
- Uma redução da superfície de ataque, eliminando a exposição de protocolos e serviços à Internet pública
- Nuvens configuradas corretamente que eliminam a forma mais comum de falha de segurança em nuvem.

Todos esses benefícios representam aspectos do nirvana da segurança que mencionamos no Capítulo 1. O Capítulo 4 analisa o retorno comercial do SSE adequado e as etapas para dar vida a ele.

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

NESTE CAPÍTULO

- Atingindo um estado de confiança adaptativa contínua usando os princípios Zero Trust
- Aprendendo os quatro passos para adotar o SSE
- Descobrindo os benefícios comerciais do SSE

Capítulo 4
Usando Zero Trust para Dar Vida ao SASE

Conforme discutimos no Capítulo 2, migrar a segurança para a nuvem é importante porque a nuvem agora é fundamentalmente importante para os negócios. A adoção da nuvem é rápida – mais rápida do que as organizações inovadoras previam há apenas cinco anos atrás. As empresas estão migrando para a nuvem para obter desenvolvimento rápido, acesso a recursos sob demanda, dimensionamento elástico e uma carga administrativa muito menor para que possam inovar e criar novos produtos e serviços em tempo recorde.

Os invasores estão migrando para a nuvem porque, bem, as empresas estão. Portanto, todos devemos nos preocupar em como garantir que nossos dados, nossas aplicações e nosso pessoal estejam seguros na nuvem.

ATENÇÃO

Se a nuvem não estiver protegida, seus benefícios permanecem inatingíveis.

Os principais responsáveis devem primeiro argumentar que proteger a nuvem é importante e, segundo, que SASE, SSE e reequipar a rede resultarão em melhor gerenciamento de risco e reduzirão o atrito de segurança. Os planos de adoção devem explicar por que essa mudança vale a pena, prever os benefícios comerciais específicos e descrever como medir esses benefícios ao longo do tempo.

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

Com base em nossas discussões sobre transformação de segurança, SASE e SSE, este capítulo descreve o caminho para o nirvana da segurança que todos desejamos, no qual nossos dados, aplicações e pessoal estejam seguros na nuvem e a criação de valor comercial substancial e inconfundível. Esse caminho agora inclui inexoravelmente a aplicação dos princípios Zero Trust à forma como arquitetamos nossa segurança.

Do Zero Trust à Confiança Adaptativa Contínua

Uma implementação bem-sucedida de SASE e SSE é mais do que trocar de tecnologia. Como explicamos no Capítulo 3, Zero Trust reformula algumas suposições básicas sobre como a segurança funciona. No modelo baseado em rede on-premises, a suposição é que a rede é segura e devemos verificar a identidade de uma pessoa antes de conceder acesso. O paradigma típico concedia ao usuário acesso a tudo ou a nada – "permitir" ou "bloquear" eram as únicas opções. Zero Trust altera este modelo da seguinte forma:

- **Quando uma pessoa solicita acesso, essa solicitação é avaliada no contexto de várias condições.** A identidade é uma delas, mas o sistema também considera onde a pessoa está, a hora do dia, o dispositivo, o tipo de conexão de rede e muitas outras variáveis.
- **A aplicação à qual a pessoa está sendo conectada faz parte desse contexto.**
- **O nível de serviço desejado é um fator importante.** Este é um uso de vida ou morte de uma aplicação ou de um videogame jogado por diversão?
- **A forma como o caminho de rede é protegido pode mudar com base no aplicação que está sendo usada.** Se alguém estiver acessando uma conta de e-mail pessoal, uma conexão comum com a Internet é usada, com a proteção Transport Layer Security (TLS) negociada entre o servidor de e-mail e o cliente de e-mail. Se um médico estiver acessando os registros do paciente, um caminho seguro, criptografado e autenticado será estabelecido, independentemente dos recursos da rede ou da aplicação subjacente.

Com base nesse contexto, o nível de confiança da sessão de uma pessoa é determinado, e pode ser concedida pouca ou muita confiança à essa pessoa. Uma pessoa solicitando acesso em um horário incomum de um

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

local incomum para uma aplicação altamente confidencial (uma instância de baixo nível de confiança) provavelmente encontrará um processo de autenticação em várias etapas. O acesso concedido pode ser limitado a um pequeno conjunto de dados e funções, e em modo somente leitura. Um funcionário que está acessando no horário habitual a partir de um local seguro (uma instância de alto nível de confiança) pode obter acesso total a todos os dados e recursos da aplicação.

Considere este exemplo de um médico acessando prontuários eletrônicos que ilustram os princípios Zero Trust em ação no SSE.

> Um médico carrega consigo um tablet de propriedade do hospital enquanto trata um paciente no hospital. Com base na identidade, localização, dispositivo e outros fatores do médico, o SSE determina que é seguro dar ao médico acesso total ao prontuário do paciente.
>
> O médico atravessa a rua para tomar um café. Ele abre um laptop pessoal, conecta-se à rede da loja e tenta acessar o prontuário do paciente. O SSE reconhece o médico, mas identifica que o notebook não é de propriedade do hospital e que o notebook está em uma rede desconhecida. O médico tem permissão para visualizar e fazer comentários no prontuário, mas não pode alterar os dados.
>
> O médico está jantando em casa; alertado sobre uma crise, ele desconecta seu filho do Minecraft para usar o PC da família para acessar o prontuário do paciente. O SSE reconhece que este computador é menos seguro que o tablet do hospital. Em vez de negar o acesso, o SSE fornece diversas perguntas que permitem que o médico verifique ainda mais sua identidade e enquadre a natureza do motivo pelo qual ele precisa de acesso. O SSE fornece ao médico um conjunto seguro de recursos para atender à emergência — por exemplo, dentro de uma sessão de navegador isolada sob controle do SSE.

Você pode estar familiarizado com o termo acesso Zero Trust à rede (Zero Trust Network Access, ZTNA). O ZTNA é uma excelente escolha para aumentar sua rede virtual privada (Virtual Private Network, VPN) para acomodar mais ambientes de acesso remoto. Com o ZTNA, os funcionários não recebem acesso à uma parte inteira de uma rede que poderia permitir conexões com muitos serviços. Em vez disso, o ZTNA concede ao funcionário uma conexão apenas com a aplicação que ele está tentando usar e – conforme mostrado na história do nosso médico – apenas o acesso mínimo necessário para realizar a tarefa em questão.

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

Se observarmos mais de perto este modelo e como ele funciona de forma mais avançada, surgem algumas ideias importantes que podem nos orientar:

- **Contexto:** na segurança pré-SASE, a rede definia o perímetro, uma barreira que precisava ser atravessada para se ter acesso. Uma certa linha de pensamento sugere que a identidade é o novo perímetro em Zero Trust porque sua identidade deve ser validada para permitir o acesso, mas este conceito é insuficiente. Uma abordagem melhor é avaliar todo o contexto, incluindo a identidade, mas também muitas outras variáveis, para determinar que tipo de acesso é permitido.
- **Privilégio mínimo:** o Zero Trust sempre tenta conceder apenas o acesso mínimo necessário para permitir que a pessoa faça seu trabalho. A forma mais avançada de Zero Trust também tenta descobrir constantemente se muitos privilégios foram concedidos e procura estreitar esse excesso de confiança do sistema.
- **Pontuação de risco:** o SSE constrói um histórico de atividades quando os funcionários interagem com as aplicações. É possível analisar este histórico para criar uma representação da atividade normal e detectar atividades suspeitas em tempo real. Esta análise gera pontuações de risco para um funcionário, para uma aplicação e para um site. Essas pontuações fornecem contexto adicional para determinar que tipo de acesso conceder.
- **Ocultação de recursos:** o acesso baseado em ZTNA não expõe endereços IP públicos aos quais qualquer pessoa pode se conectar. A conectividade é possível somente após o contexto ter sido avaliado. Por padrão, tudo está oculto. (Sim, há um papel para a obscuridade na segurança, ao contrário do que é frequentemente ensinado nas aulas de segurança da informação.)
- **Confiança adaptativa contínua (provavelmente a maior ideia desta lista):** confiança adaptativa contínua é a prática de monitorar uma conexão e ajustar constantemente as permissões com base nas mudanças no contexto. Uma pessoa que normalmente usava o Salesforce está tentando acessar o sistema de tesouraria do CFO? Sinal de alerta: reduza o acesso e a autorização, aumente a pontuação de risco e alerte alguém para agir. Outra pessoa está tentando acessar um site perigoso? Exiba uma janela com um aviso antes de conceder acesso. O objetivo é reagir constantemente às mudanças no contexto para proteger adequadamente os dados, as aplicações e as pessoas.

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

LEMBRAR

A implementação do SSE com princípios Zero Trust reduz a superfície de ataque e é muito mais baseada em dados, melhorando muito a postura geral de segurança. Conforme o nível de risco apresentado por uma pessoa, uma aplicação ou um site é constantemente reavaliado, a segurança se adapta em tempo real com base nas mudanças no contexto.

Agora, com nossa mentalidade de confiança adaptativa contínua firmemente estabelecida, podemos passar para uma discussão sobre como implementar o SSE da maneira certa.

Quatro Etapas Simples para o SSE

Dar vida ao SSE para a maioria das organizações envolve passar da segurança on-premises tendo a rede como perímetro para a segurança na nuvem tendo o contexto como perímetro. Vamos supor um ponto de partida que reflita onde se encontra a maioria das empresas no momento – um firewall on-premises que inclui VPNs para acesso remoto, um secure web gateway (SWG) on-premises que controla o acesso à Web e talvez uma assinatura para um agente de segurança de acesso à nuvem (Cloud Access Security Broker, CASB) autônomo que protege o uso de aplicações SaaS.

1ªEtapa: Migrar trabalhadores móveis para recuperar a visibilidade

A primeira coisa a fazer é avaliar o que seus funcionários estão fazendo e medir seu nível atual de risco. A maneira mais fácil de fazer isso é começar com sua população de usuários móveis, porque esses funcionários apresentam potencialmente mais riscos. Direcione o tráfego da Web e do SaaS por meio dos recursos SWG e CASB do SSE, configurados o mais próximo possível das políticas existentes. Depois observe.

Este exercício gera uma visão mais completa do que os funcionários estão fazendo. As empresas que ainda não usam CASB ou SWG descobrirão uma quantidade enorme (e potencialmente alarmante) de atividades. As empresas que já estão usando CASB e SWG também aprenderão mais.

Você certamente descobrirá que os trabalhadores móveis estão acessando aplicações e serviços que você não sabia. Você aprenderá onde eles estão trabalhando e que tipo de redes eles tendem a usar.

A parte restante da primeira etapa é migrar o acesso a sistemas internos no data center de VPNs para o ZTNA no SSE. Isso melhora a experiência do funcionário e aumenta a segurança ao mesmo tempo. Imagine que

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

um encanador vem à sua casa para consertar um vazamento enquanto você está no trabalho. Ele tem acesso à toda a sua propriedade no caminho de ida e volta entre o caminhão dele e o seu banheiro. Talvez ele deixe a porta da frente aberta. Durante todo esse tempo, você não tem ideia do que está acontecendo. O ZTNA é como se armar com um botão mágico de teletransporte. O encanador aparece, você o teletransporta do caminhão para o vazamento e depois de volta para o caminhão sem paradas no meio. É o controle de acesso, aperfeiçoado para a era da nuvem.

2ª Etapa: Migrar os funcionários restantes e aplicar a classificação de dados em toda a empresa

A segunda etapa é migrar todos seus funcionários locais sob a proteção do SSE para controlar o acesso a aplicações e a serviços em nuvem. Realizar esta etapa para que todos os funcionários, tanto locais quanto móveis, sejam protegidos pelo SSE, transforma sua arquitetura de rede. Todos os funcionários agora atravessam o ponto de presença mais próximo do provedor de SSE, que então roteia o tráfego para o destino de maneira otimizada – geralmente com menos saltos do que a Internet pública. Agora, você pode simplificar a rede e aposentar redes privadas dispendiosas que podem não ser mais necessárias. Como parte dessa transição de rede, a rede de longa distância definida por software (Software-Defined Wide-Area Networking, SD-WAN) pode ser introduzida para direcionar seletivamente o tráfego das filiais.

O objetivo é obter uma compreensão completa dos dados, aplicações, sites e outros serviços de interesse dos nossos funcionários. Nesta etapa, o poder do SSE para capturar e analisar a atividade aumenta drasticamente o escopo e a profundidade do contexto. A postura de segurança expressa por suas políticas de SSE nesta etapa provavelmente deve ser semelhante àquelas já presentes em quaisquer produtos legados que o SSE esteja substituindo. É importante corresponder a um estado conhecido antes de adicionar novos recursos que podem exigir instrução e treinamento.

Com esse novo contexto em mãos, você pode estabelecer as bases para uma melhor segurança classificando dados, aplicações e pessoas com base em risco e comportamento. Com esta classificação concluída, o sistema SSE pode usar dados internos e externos para calcular pontuações de risco em tempo real para funcionários, aplicações e sites. Agora é

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

possível aposentar grande parte da infraestrutura de segurança legada e passar para a próxima etapa em que o SSE passa para um novo nível de segurança.

3ª Etapa: Implementar confiança adaptativa contínua e serviços ampliados

Até este ponto, a experiência dos funcionários não mudou muito. Na 3ª Etapa, a experiência muda significativamente porque a segurança se adapta com base no contexto.

LEMBRAR

A confiança adaptativa contínua avalia o contexto para equilibrar o risco com a confiança, fornecendo o tipo correto de acesso a qualquer momento. Ela permite que você defina políticas de segurança muito mais detalhadas. Além disso, ela cria com mais frequência avisos ou sugestões quando as pessoas estão prestes a fazer algo perigoso, ajudando a orientar os funcionários para as ações aprovadas.

Com o SSE, os profissionais de segurança sabem quais dados são confidenciais e quais aplicações e sites são arriscados. Reunir este sentido com recursos como o DLP permite que a equipe de segurança controle o que as pessoas fazem com dados confidenciais de maneira detalhada – em um nível sem precedentes em termos de segurança. Em vez de um simples bloqueio ou decisão de permissão, o acesso cai em um continuum.

A confiança adaptativa contínua também permite adicionar mais serviços. Por exemplo, digamos que um médico queira visitar um site considerado arriscado. Após um aviso, o médico ainda quer visitá-lo. O SSE poderia então desviar o médico para uma sessão de isolamento de navegador remoto (RBI), um navegador que é executado em uma máquina virtual no provedor do SSE, o que reduz ainda mais o risco. Outros serviços avançados podem ser adicionados conforme necessário.

4ª Etapa: Gerencie o risco proativamente com análise e pontuação dinâmicas

Na 4ª Etapa, a equipe que opera o SSE pode iniciar o processo de descoberta proativa de riscos e eliminá-los do ambiente. Um método para medir o progresso é rastrear as pontuações de risco de funcionários, aplicações e sites. O objetivo é mostrar uma redução na quantidade de tráfego para sites de risco e uma redução na frequência de ações arriscadas. Outro método é reduzir os direitos, rastreando os padrões de uso e eliminando o excesso de privilégios.

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

Neste momento, alguns dos controles de segurança de nível superior, como DLP e neutralização de ameaças, podem se tornar o foco, aumentando os recursos de CASB, SWG, ZTNA e firewall como serviço (FWaaS). No SSE, esses controles funcionam melhor do que em suas versões on-premises separadas e muito mais pode ser feito com eles. Por exemplo, os reconhecedores baseados em aprendizado de máquina permitem que o DLP identifique e reaja a documentos confidenciais em tempo real.

DICA

O gerenciamento de experiência digital (DEM), o gerenciamento de postura de segurança na nuvem (CSPM) e o gerenciamento de postura de segurança SaaS (SSPM) melhoram ainda mais o gerenciamento de riscos. Eles adicionam métodos avançados para garantir disponibilidade e desempenho consistentes e para localizar e corrigir erros de configuração. O SSE permitirá serviços ainda mais avançados no futuro.

LEMBRAR

Sua situação específica ditará os detalhes à medida que você trabalhar em cada etapa. Mas a partir de um alto nível, as etapas explicam o processo pelo qual a maioria das empresas passará para implementar totalmente o SSE.

Transformando a Rede e o Resto da Segurança

DICA

A implementação do SSE é uma etapa importante e inegociável para o SASE. Mas para alcançar o nirvana da segurança que almejamos, o restante do ambiente de segurança além do SASE também deve evoluir para que todas as partes importantes trabalhem juntas. A maioria das empresas está mudando para um modelo de "trabalho em qualquer lugar", no qual os benefícios da segurança em qualquer lugar e a qualquer hora são claros. Isso naturalmente se afasta da conectividade baseada em VPN e da rede privada, e oferece a simplicidade e as vantagens de custo do SSE.

A questão mais importante a ser lembrada é, ao adotar o SSE (e o SASE), como a infraestrutura geral de tecnologia se torna mais simples. No modelo antigo, controles de segurança para proteção contra acesso não autorizado eram colocados na rede corporativa porque essa rede era o único caminho para os dados. No novo modelo, os vários pontos de presença do provedor do SSE tornam-se os caminhos para os dados, oferecendo não apenas controle de acesso, mas também inspeção completa de tráfego. A rede subjacente pode então se concentrar na sua missão geral de migrar bits de dados de maneira rápida e eficiente.

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

Os sistemas de gerenciamento de identidade e acesso (Identity and Access Management, IAM) realizam o importante trabalho de autenticar funcionários. Muitos desses sistemas já são altamente configuráveis por meio de interfaces de programação de aplicações (APIs). Eles também são projetados para integração com outros sistemas, um recurso necessário para qualquer implementação de SSE. As melhorias em tecnologia de IAM fornecem ainda mais contexto, monitoramento e recursos avançados de autenticação dos quais o SASE e o SSE podem se beneficiar. O SSE obtém ainda mais benefícios das plataformas de proteção de terminais (Endpoint Protection Platform, EPP). Ele coleta sinais importantes (gerando assim mais contexto), realiza monitoramento detalhado e inclui mecanismos para controlar o comportamento e a configuração de segurança. Sincronize seu plano de implementação do SSE com uma evolução de EPP correspondente para obter o máximo valor de seus investimentos em segurança.

O SASE e o SSE irão acelerar a mudança no papel do data center. Depois que a nuvem ganhou destaque, o data center perdeu sua posição como foco das atividades relacionadas à segurança. O SSE transfere a segurança do data center para a nuvem.

LEMBRAR

Os data centers ainda desempenharão um papel importante na maioria das empresas por vários bons motivos, como pressões de custo, requisitos regulatórios, gerenciamento de risco e a conveniência de ter tipos especiais de infraestrutura de computação. Agora, o data center será um dos muitos locais onde aplicações importantes são hospedadas e protegidas pelo SSE.

Benefícios Comerciais do SSE

O risco cibernético é uma prioridade para a maioria das diretorias, mas como deixamos claro no Capítulo 2, a segurança não é um fim em si mesma. Ela tem a missão de proteger o valor comercial que está sendo criado pelos sistemas que sustentam o negócio. As empresas migraram para a nuvem porque faz sentido para os negócios. O trabalho de uma arquitetura SASE, incluindo o SSE, é proteger aplicações, dados e pessoas. Veja como isso se traduz em valor comercial:

- **A segurança não atrapalha mais a produtividade dos negócios.** A agilidade comercial pode ser apoiada e as equipes de segurança não precisam mais desempenhar o papel de Dr. Não, porque os movimentos que a empresa deseja fazer agora podem ser devidamente protegidos. O atrito induzido pela segurança é reduzido drasticamente. Os processos de desenvolvimento e de

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

manutenção de produtos são simplificados à medida que a segurança é incorporada mais facilmente. Um SSE em nuvem é perfeitamente adequado para proteger um ambiente em várias nuvens.

- **A diretoria agora tem muito mais confiança de que os tipos de controle necessários para usar com segurança os recursos da nuvem estão sendo examinados e gerenciados adequadamente.** O processo de gerenciamento de riscos relacionados a pessoas, dados e aplicações torna-se muito mais sofisticado, assim como os mecanismos usados para mitigar riscos. Com o SSE, o risco pode ser identificado de forma proativa e sistematicamente eliminado de uma empresa. A segurança em um sentido real acompanha os dados, o que proporciona uma sensação de tranquilidade à diretoria sobre o nível de proteção dos os ativos mais importantes.
- **A equipe de segurança se torna muito mais unificada e focada nos negócios.** Em vez de precisar de um funcionário para SWG, um funcionário para CASB e um funcionário para o firewall, você tem uma equipe focada no panorama geral com mais informações para ser proativa.

LEMBRAR

Dar vida ao SSE significa dar vida a um mundo de segurança muito melhor, e todos os envolvidos na empresa encontrarão um benefício.

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

Capítulo 5
Dez (ou Mais) Dicas do que Fazer e do que Não Fazer na Jornada Rumo ao SSE

Uma grande parte em concluir a jornada rumo à uma nuvem segura e ágil é reconhecer que sua organização de TI atual não foi projetada para esse destino. É natural que a organização de TI reflita a arquitetura de tecnologia. Portanto, se indivíduos ou equipes distintos cuidarem de seus agente de segurança de acesso à nuvem (CASBs), seus secure web gateways (SWGs), suas rede virtual privada (VPNs) e seus firewalls, juntamente ou como parte de um centro de operações de segurança (Security Operations Center, SOC) e uma equipe do centro de operações de rede (Network Operations Center, NOC), você enfrentará resistência quando disser: "Ei, agora vamos implementar uma nova arquitetura integrada de Secure Access Service Edge (SASE) e de Security Service Edge (SSE) que também converge segurança e rede em um poderoso exército." As pessoas naturalmente resistem à mudança, em parte por medo de perder o controle de um domínio que trabalharam duro para entender completamente.

O SASE e o SSE oferecem benefícios táticos que melhoram a qualidade da segurança e expandem o alcance dos serviços de segurança e os benefícios estratégicos que podem acelerar os negócios. As seções a seguir fornecem um guia para ter sucesso com a adoção do SASE e do SSE. Primeiramente, apresentamos quatro princípios para acelerar sua jornada. Em seguida, sugerimos quatro erros a serem evitados.

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

Faça dos Dados o Foco

Sob o SSE, a segurança acompanha os dados onde quer que eles forem. Portanto, não importa se você está criando dados no Google Workspace e no Microsoft 365, em uma aplicação de software como serviço (SaaS) ou no armazenamento de objetos em nuvem. O SSE está sempre lá para proteger esses dados.

Como o SSE se torna um ponto de inspeção primário que também pode facilitar a classificação de dados, é importante determinar a finalidade e a localização de todos os seus dados. Use esse conhecimento para priorizar a proteção e o uso adequado de dados confidenciais onde quer que estejam, para que você possa ter certeza de que fez o trabalho mais importante primeiro.

Adote a Integração

Em cada etapa do ciclo de resposta a incidentes, é importante desenvolver habilidades de automação e de integração para que você possa convergir seus componentes de segurança em uma máquina bem ajustada. O processo envolve extrair informações de vários sistemas, integrar essas informações para analisar o que está acontecendo, montar a equipe certa e tomar medidas automatizadas quando possível.

O SSE integra os serviços de segurança cruciais para proteger a nuvem, mas vive como parte de um ecossistema maior de serviços de segurança importantes. Sistemas de gerenciamento de identidade e acesso (IAM), plataformas de proteção de terminais (EPP) e ferramentas de informações de segurança e gerenciamento de eventos (Security Information and Event Management, SIEM) são alguns dos principais componentes que trabalham em conjunto com funções específicas do SSE para fornecer segurança abrangente e apoiar o diagnóstico rápido e a resposta a problemas.

Lembre-se de que os Malfeitores Também Estão na Nuvem

O SSE e o SASE representam um grande avanço no escopo e na qualidade da segurança. É razoável sentir-se satisfeito depois de fazer os princípios básicos funcionarem. Mas lembre-se, os invasores também usam a nuvem para melhorar suas habilidades. A porcentagem de malwares entregues por meio de aplicações em nuvem aumentou de 50% no segundo trimestre de 2020 para um recorde histórico de 68%

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

no segundo trimestre de 2021, de acordo com o Cloud and Threat Report da Netskope (www.netskope.com/blog/july-2021-netskope-cloud-and-threat-report). O SSE o impulsiona à frente dos malfeitores, mas você deve estar constantemente aprendendo e se adaptando para permanecer à frente.

Reconheça que a Segurança É uma Parte Fundamental da Estratégia de Negócios

A segurança deve fazer parte de uma discussão da estratégia de negócios desde o início. Ficar empolgado com as aplicações e a nuvem não faz sentido se essas aplicações e as pessoas que trabalham com elas não puderem ser protegidas. A boa notícia é que o SSE ajudará as equipes de segurança a se tornarem mais facilmente um facilitador de negócios. Se a equipe de segurança entender as metas de negócios e suas ramificações de segurança, a equipe poderá dizer "sim" com mais frequência porque tem mais poder para proteger qualquer coisa que a empresa queira fazer.

DICA

Para que a adoção do SASE e do SSE seja bem-sucedida, os promotores do programa devem explicar que os benefícios de proteger a nuvem são importantes no nível da grande estratégia comercial. A mensagem: Investimos na nuvem para transformar nossos negócios e criar melhores resultados. Agora, devemos proteger esse investimento. A empolgação em alcançar e proteger esses resultados será a melhor motivação para adotar com entusiasmo o SASE e o SSE.

Não Pense em Silos

O SASE e o SSE resolvem os problemas complexos que costumam acompanhar os projetos de nuvem. Evite tentativas de implementar CASB, SWG e acesso Zero Trust à rede (ZTNA) como projetos independentes, o que adiciona mais provedores de nicho prometendo mais distrações. O objetivo é proteger a nuvem com uma plataforma integrada com reconhecimento de contexto. Haverá resistência à mudança que o SASE e o SSE implicam.

ATENÇÃO

Um grande erro é desacelerar o processo, abordando o problema a partir de silos convencionais de TI. Esses "cilindros de excelência" perpetuam velhas formas de pensar no novo mundo. A segurança não deve mais ser categorizada apenas como um problema de rede. Não tenha uma conversa sobre rede para um problema de segurança. Agora, o SSE se tornou o ponto de controle e visibilidade de segurança fundamental como parte de uma arquitetura SASE totalmente funcional.

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

Não Transfira Regras Antigas

As pessoas geralmente têm medo de seus firewalls porque acumularam camadas de regras criadas por pessoas que partiram há muito tempo. O mesmo pode ser verdade para outras tecnologias de segurança que exigem regras complexas e definições de configuração para alcançar os resultados desejados. O SSE é diferente. Embora as regras e a configuração ainda existam, grande parte do trabalho é realizado com a definição de políticas que descrevem os resultados. Quando implementado de forma eficaz, o SSE gerencia os detalhes das interações de regras por conta própria. Portanto, não se preocupe com a configuração da sua tecnologia antiga. Em vez disso, concentre-se nos resultados de segurança desejados e use o SSE para alcançá-los.

A maioria dos produtos de SSE também oferece gerenciamento de postura de segurança na nuvem e gerenciamento de postura de segurança SaaS para ajudá-lo a acertar e manter o bom funcionamento.

Não Odeie o Data Center

Agora que você está adotando o SASE e o SSE, é fácil achar que o data center tradicional não é importante. Sempre teremos data centers de alguma forma; afinal, a nuvem nada mais é do que um conjunto de data centers com acesso por meio de interfaces de programação de aplicações (APIs). A nova finalidade do data center é um local para importantes cargas de trabalho e aplicações de computação. O data center não é mais o papel principal na infraestrutura de segurança, mas ainda desempenha um importante papel de suporte.

Não Tenha Medo de Mudanças

Não deixe o medo do SASE e do SSE atrapalhar o seu objetivo final. Sim, há uma mudança na arquitetura e novos produtos para entender, uma tarefa difícil porque os produtos interagem com todos na empresa. Uma implementação de SSE ensinará mais sobre seu pessoal, seus dados, suas aplicações e seus sites e aplicações de terceiros. Esse conhecimento, então, abrirá as portas para mais automação para encontrar erros e implementar respostas eficazes. Comparado com sua atual postura de segurança, viver no novo mundo parecerá o nirvana.

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

SSE é a pilha de segurança que determinará uma arquitetura SASE bem-sucedida. Este livro mostra como alcançar o SSE hoje.

A jornada do SASE requer parceiros confiáveis com recursos de plataforma verdadeiramente integrados, não provedores com marketing apelativo proclamando "SASE" ou "SSE" em letras gigantes. Este livro é o seu guia prático para SSE e SASE, incluindo por que ambos os conceitos são tão fundamentais para criar arquiteturas de segurança e rede centradas na nuvem do futuro e como investir e projetar para Security Service Edge (SSE) hoje.

Tópicos deste livro...

- Defina SASE e SSE
- Aprenda o papel essencial da Zero Trust
- Proteja dados comerciais valiosos na nuvem
- Turbine sua força de trabalho em qualquer lugar
- Evite armadilhas de projeto para SSE e SASE

netskope

Os líderes da Netskope, **Jason Clark** (CSO e CMO) e **Steve Riley** (CTO de campo) são autoridades amplamente reconhecidas em tecnologia de computação em nuvem, segurança cibernética e redes, com décadas de experiência em organizações globais, incluindo Gartner, Optiv, Riverbed e Websense.

Acesse Dummies.com®
para ver vídeos, fotos passo a passo, artigos de instruções ou para fazer compras!

ISBN: 978-1-119-89665-4
Proibida a revenda

para leigos®

WILEY END USER LICENSE AGREEMENT

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