

APRENDIZADO FACILITADO



Edição especial da
Netskope

Segurança de Dados Unificada

para
leigos
A Wiley Brand



Modernize a
segurança dos
seus dados

Proteja seus dados onde
quer que eles estejam ou
se movam

Minimize falsos
positivos

Trazido para
você por:

 **netskope**

Sobre a Netskope

A Netskope, líder em segurança e redes modernas, atende às necessidades das equipes de segurança e de redes, oferecendo acesso otimizado e segurança em tempo real, baseada em contexto, para pessoas, dispositivos e dados onde quer que estejam. Milhares de clientes, incluindo mais de 30 empresas da Fortune 100, confiam na plataforma Netskope One, em seu Zero Trust Engine e na poderosa rede NewEdge para reduzir riscos e obter total visibilidade e controle sobre aplicações de nuvem, IA, SaaS, web e privadas — oferecendo segurança e acelerando o desempenho sem comprometimentos.

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

Da Netskope: Ankur Chadda, Tom Baumgartner, Ramien Ebadypour, Emily Wearmouth, Kathy Jacobsen, Stephenie Pang



Segurança de Dados Unificada

Edição especial da Netskope

para
leigos[®]
A Wiley Brand

Segurança de Dados Unificada Para Leigos®, edição especial da Netskope

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

Direitos autorais © 2026 por John Wiley & Sons, Inc., Hoboken, Nova Jersey. Todos os direitos, incluindo mineração de texto e dados, treinamento de IA e tecnologias semelhantes, são reservados.

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, Para Leigos, 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 outras marcas comerciais pertencem a seus respectivos proprietários. A John Wiley & Sons, Inc. não está associada a nenhum produto ou fornecedor mencionado neste livro.

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

Para obter informações gerais sobre nossos outros produtos e serviços, ou sobre como criar um livro personalizado *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.dummies.com/custom-solutions. 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 978-1-394-42070-4 (pbk), ISBN 978-1-394-42071-1 (ebk), ISBN 978-1-394-42072-8 (ebk)

Agradecimentos da editora

Editor: Elizabeth Kuball

**Responsável por
aquisições:** Traci Martin

Editor gerente sênior: Rev Mengle

**Gerente de contas de
clientes:** Jeremith Coward

**Responsável pela
produção:** Magesh Elangovan

Contribuição especial: Joe Kraynak

Introdução

A segurança de dados como um conceito em segurança cibernética não é nova, mas as demandas impostas aos sistemas legados de segurança de dados mudaram drasticamente na última década. Os profissionais de segurança já estiveram confiantes de que os dados valiosos que protegiam estavam guardados em data centers fortemente protegidos. Mas a transformação digital implica que as empresas, grandes e pequenas, movam seus dados para a nuvem e em locais distribuídos. Seus dados agora estão presentes em qualquer lugar que os usuários estejam. Sua empresa pode compartilhar conexões digitais com um grande número de fornecedores, parceiros e prestadores de serviços terceirizados e até mesmo quarteirizados. Esses cenários trazem oportunidades de negócios sem precedentes (boas notícias) e desafios de segurança, principalmente no que diz respeito à segurança de dados (más notícias).

Violações bem-sucedidas podem ter consequências devastadoras para a empresa. Os riscos de pessoas internas (sejam mal-intencionadas ou negligentes) são tão perigosos para o seu negócio quanto os ataques de agentes externos que dominam as manchetes. Todos eles ameaçam expor informações confidenciais. A segurança de dados agora é a base das regras de conformidade, com regulamentos de privacidade de dados e do setor que detalham especificamente as responsabilidades da empresa e impõem penalidades significativas por falhas.

As empresas devem adotar uma nova abordagem e aplicar políticas de segurança de dados em todos os lugares onde seus dados vão — de forma consistente. O ideal é que a segurança de dados apoie os objetivos do negócio e, ao mesmo tempo, proteja a empresa. Mas gerenciar políticas de segurança de dados e as ferramentas necessárias para aplicá-las pode ser complexo e caro. As organizações precisam de soluções de segurança de dados que simplifiquem a imposição de políticas e, ao mesmo tempo, garantam a eficácia das políticas. Uma nova geração de soluções de gerenciamento de postura de segurança de dados (DSPM) e prevenção de perda de dados (DLP) entregues na nuvem oferece um caminho a seguir. As organizações devem adotar uma solução fornecida em nuvem que seja menos complexa, altamente escalável e mais econômica enquanto, de preferência, protege os dados com maior confiabilidade e melhor precisão e minimiza a exposição a acesso não autorizado ou uso indevido. É um equilíbrio difícil de encontrar, mas você pode alcançá-lo hoje com a orientação certa.

Sobre este Livro

Este livro pode prepará-lo para tomar decisões bem informadas sobre como avaliar a abordagem atual de sua organização para segurança de dados e avaliar novas soluções para encontrar a melhor escolha para suas necessidades, usando princípios zero trust para orientar como a segurança é aplicada de forma contextual e consistente. Ao explicar como funcionam os sistemas modernos de DSPM e DLP entregues na nuvem, este livro vai além do apelo publicitário ao identificar as características e os recursos necessários para proteger de forma confiável seus dados onde quer que residam e se movam.

Suposições Tolas

Este livro pressupõe que você tenha um conhecimento básico de como as empresas adotaram o uso da computação em nuvem para se tornarem flexíveis e melhor equipadas para adotar a transformação digital. Também pressupõe que você está aqui porque deseja garantir a combinação certa de tecnologia e melhorias de processo para proteger dados confidenciais onde quer que residam e onde quer que se movam em seu ambiente de computação.

Ícones usados no livro

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



DICA

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



LEMBRE-SE

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

Embora este livro esteja repleto de informações, se ao final você pensar: “Onde posso aprender mais?”, acesse www.netskope.com.

NESTE CAPÍTULO

- » Compreendendo onde os dados confidenciais são armazenados e como são monitorados
- » Descobrindo o que é realmente a segurança de dados
- » Aprendendo sobre DSPM e DLP
- » Investigando por que a DLP legada, sozinha, não é mais uma solução viável
- » Migrando para uma estratégia focada em nuvem com uma solução unificada de segurança de dados
- » Derrubando mitos comuns sobre DLP

Capítulo 1

Revisando os princípios básicos de segurança de dados

A digitalização de dados tornou muito mais fácil acessar, usar, alterar e compartilhar, mas muito mais difícil monitorar e proteger. Este capítulo coloca você a par dos fundamentos da segurança de dados e dos desafios emergentes, além de revelar os fatos por trás dos mitos que cercam a DLP (data loss prevention).

Um Guia Rápido sobre Dados Confidenciais

Você pode perceber que a maioria dos dados rotulados como confidenciais existe de alguma forma há anos, décadas ou até mais tempo:

- » **Dados pessoais**, como números de CPF, números de cartão de crédito, números de carteira de motorista, informações de saúde e endereços residenciais
- » **Propriedade intelectual**, como designs de produtos, novas invenções, patentes e código-fonte

» **Informações confidenciais e segredos comerciais**, como planejamentos financeiros, contratos, relatórios fiscais, informações sobre fusões e aquisições, e documentos de pré-lançamento como comunicados à imprensa

A novidade é que o cenário empresarial moderno mudou completamente a forma como os dados são compartilhados e (ai ai ai!) expostos. Quase todos os tipos de dados confidenciais são criados, armazenados e movidos digitalmente. Os dados vão e voltam de serviços em nuvem, redes corporativas e qualquer outro lugar onde os usuários possam acessá-los. Ao mesmo tempo, um número cada vez maior de aplicações armazena e compartilha esses dados em várias plataformas, tornando-as acessíveis de praticamente qualquer dispositivo em qualquer local remoto. Para agravar o problema, muitas empresas agora adotam um ambiente de trabalho híbrido.

À medida que a quantidade, a variedade e a velocidade dos dados aumentam exponencialmente, torna-se cada vez mais difícil identificar e proteger informações confidenciais. Para piorar a situação, o grande volume de dados disponíveis dificulta que as medidas de segurança tradicionais acompanhem as ameaças emergentes.



LEMBRE-SE

Em geral, quando as pessoas falam sobre dados sensíveis, elas estão se referindo a informações confidenciais ou pessoais. O que é confidencial depende muito se você olha para os dados de uma perspectiva comercial ou de uma perspectiva individual.

Um Maremoto de Dados

Até 2028, de acordo com a Statista, o mundo estará inundado com até 394 zettabytes de dados! Uma grande parte desses dados será criada e armazenada diretamente na nuvem – aumentando a cada ano que passa. Entre os desafios que os sistemas de proteção de dados e seus operadores enfrentam estão

» **Aumento de categorias de dados confidenciais:** um aumento nas regulamentações e leis de privacidade de dados que protegem uma ampla variedade de indivíduos e tipos de informações em todo o mundo está impulsionando um crescimento maciço nas categorias de dados confidenciais. Isso inclui informações que podem identificar uma pessoa, como a localização, suas informações financeiras e de saúde, preferências pessoais, crenças religiosas e orientação sexual. Os dados confidenciais incluem coisas como números de identidade, números de cartão de crédito, código-fonte, projetos, planos

financeiros, contas bancárias, contratos, formulários de impostos, senhas, informações de fusões e aquisições, informações de saúde protegidas (PHI), e-mail confidencial, sexo e religião. Existem categorias de dados confidenciais que diferem de país para país, em idiomas localizados e que são específicos para cada país.

- » **Aumento de formatos e tipos de dados:** isso inclui PDFs, imagens gráficas (como JPG, PNG e BMP), arquivos de vídeo (como MP4, MOV e AVI), arquivos compactados e encapsulados (como ZIP, RAR e ISO), anexos, mensagens do Slack, bate-papos, formulários on-line, capturas de tela, planilhas, CAD (computer-aided design), postagens sociais, arquivos de texto, apresentações e e-mails.
- » **Contexto em expansão:** o contexto deve governar uma decisão sobre como os dados confidenciais devem ser acessados, usados, transferidos e compartilhados com segurança. O contexto ajuda a definir o que seria uma ação arriscada em torno de dados confidenciais e o que deveria ser considerado uma violação ou tentativa de violação: quem, onde, o que, como, por que, quando, para quem e outros fatores.

Diante de uma onda de dados inescrutáveis, os sistemas de segurança legados são forçados a pecar por excesso de cautela, o que aumentou as dores de cabeça administrativas em grande magnitude. Por quê? As equipes de segurança de resposta a incidentes enfrentam enxurradas de falsos positivos, a maioria dos quais deve ser avaliada manualmente por funcionários já sobrecarregados.

A segurança de dados é muito mais do que “apenas” dados

As empresas precisam de novas estratégias automatizadas que possam identificar, monitorar e proteger com eficácia seus dados valiosos. Ao mesmo tempo, o mundo em que opera a segurança de dados continua a apresentar novos desafios que agravam a crise de segurança. Esses novos desafios incluem o seguinte:

- » **Mais riscos cibernéticos:** as empresas enfrentam mais vulnerabilidades a violações de dados do que nunca. Essas vulnerabilidades podem ser intencionais e não intencionais. O comportamento interno, como funcionários roubando ou manuseando dados de forma incorreta (opal), é uma das formas pelas quais as informações confidenciais de uma empresa correm o risco de exploração. Oitenta e dois por cento das violações de dados envolvem o elemento humano, que inclui

- *Pessoas mal-intencionadas*: por exemplo, um funcionário insatisfeito fazendo capturas de tela de uma planilha importante, enviando dados para uma instância de uma aplicação SaaS (software as a service) de armazenamento pessoal ou por meio de uma instância pessoal de uma conta de e-mail corporativa (por exemplo, Gmail pessoal em vez de Gmail corporativo).
- *Exposição não intencional*: por exemplo, um funcionário que inadvertidamente envia muitas informações a um fornecedor ou compartilha arquivos em excesso de forma negligente em uma pasta do Microsoft OneDrive. Essas são causas significativas de violações de dados.

Da mesma forma, ataques externos ou tentativas de invasão também colocam os segredos da empresa em risco de serem exigidos resgate ou revelados ao público ou a organizações rivais.

» **Nuvem, incluindo SaaS e IaaS (infrastructure as a service) de nuvem pública:** a adoção de aplicações SaaS, em particular, está aumentando em um ritmo impressionante. De acordo com estudos recentes, uma empresa usa em média mais de 2.400 aplicações em nuvem, com 97 por cento considerado *shadow IT* (não sancionado, desconhecido ou invisível para o departamento de TI). Isso apresenta desafios técnicos e de segurança porque os dados podem ser armazenados e compartilhados em um grande número de aplicações SaaS, desloca-se por redes corporativas e dispositivos gerenciados e podem ser facilmente acessados por funcionários e até mesmo por usuários externos conectados em locais remotos com dispositivos não gerenciados. As aplicações em nuvem podem rapidamente se tornar um vetor de ataque primário se não forem monitoradas e gerenciadas adequadamente. As empresas devem tomar medidas para atualizar suas soluções de proteção de dados para se proteger contra essas ameaças.

» **Trabalho híbrido:** a ascensão da força de trabalho híbrida está mudando a forma como as empresas armazenam e acessam dados confidenciais. As práticas empresariais atuais são drasticamente diferentes dos dias em que as empresas mantinham as informações mais importantes em um data center privado sobre o qual a empresa tinha controle. A força de trabalho híbrida trouxe uma nova era em que os dados confidenciais são altamente distribuídos em locais além das fronteiras corporativas que a empresa não pode ver e não controla. Hoje em dia, os dados estão espalhados por uma variedade de ambientes, tanto digitais quanto físicos, incluindo data centers, locais de trabalho da sede corporativa, filiais, home offices e dispositivos de trabalhadores remotos (corporativos e pessoais).

- » **Novos requisitos de conformidade:** A conformidade sempre foi uma preocupação, mas à medida que as empresas se tornam mais regulamentadas e a legislação de privacidade de dados acarreta multas e ações legais cada vez mais pesadas, empresas de todos os tamanhos estão sentindo a pressão para atender aos padrões de conformidade e proteger seus dados confidenciais, bem como os de seus clientes e parceiros. As empresas devem tomar medidas para atender às regulamentações de todo o setor, como o PCI DSS (Payment Card Industry Data Security Standard), o HIPAA (Health Insurance Portability and Accountability Act) e o GLBA (Gramm–Leach–Bliley Act), ao mesmo tempo, garantindo que cumpram as leis e os regulamentos de privacidade de dados aplicáveis, incluindo o RGPD (Regulamento Geral de Proteção de Dados) da União Europeia, a CCPA (California Consumer Privacy Act), a Lei de Privacidade do Colorado, a Lei de Privacidade de Dados de Connecticut, a Lei de Proteção de Dados do Consumidor da Virgínia, e a Lei de Privacidade do Consumidor de Utah, para citar apenas alguns. Muitos países ao redor do mundo são regulamentados por leis de privacidade, incluindo Brasil, Japão, Cingapura e Reino Unido. Agora, mais do que nunca, as empresas precisam mostrar que estão tomando as medidas necessárias para proteger as informações pessoais de seus clientes e agir de acordo com todas as políticas legislativas relevantes ou correm o risco de sofrer penalidades severas.
- » **Talento raro e caro:** o talento especializado e qualificado necessário para executar programas complexos de segurança de dados é escasso. As tecnologias de segurança de dados exigem supervisão hábil para lidar com grandes quantidades de incidentes acionados pelo sistema. Esse problema aumenta quando os sistemas legados de proteção de dados monitoram serviços em nuvem como aplicações SaaS (algo para o qual não foram projetados inicialmente), causando uma maior ocorrência de falsos positivos e, como resultado, muito trabalho adicional para a equipe. Com base nos conjuntos de habilidades necessárias, essa equipe de TI qualificada recebe altos salários, o que pode representar um custo elevado para as empresas – quer permaneçam e devam ser pagos, quer fiquem sobrecarregados, saiam e precisem ser substituídos.

O que é segurança de dados unificada e como ela pode ajudar?

A segurança de dados unificada combina o melhor DSPM (data security posture management) e DLP para reduzir custos e complexidade, tudo em um único painel de controle.

A tecnologia DSPM fornece um processo e uma estrutura que ajuda as organizações a gerenciar e aprimorar proativamente a segurança de seus dados, tanto no local quanto na nuvem. Ela consegue isso identificando, avaliando e mitigando riscos relacionados a dados, incluindo vazamento de dados, e garantindo a conformidade regulatória. Isso dá aos líderes e profissionais de segurança da informação visibilidade total sobre quais dados sua organização possui, onde esses dados estão, quem tem acesso a eles e os riscos que as interações com esses dados apresentam. O DSPM gerencia riscos em todo o ciclo de vida dos dados, com descoberta, classificação e marcação automatizadas de dados, criação de perfis de usuários para privilégios e acesso, rastreamento de exfiltrações de dados e violações de políticas, correção e aumento de privilégios automatizados e geração de relatórios.

As tecnologias de segurança de DLP são sistemas projetados para descobrir e proteger automaticamente o armazenamento, o fluxo e o uso de dados confidenciais, seja nas redes, ou através de usuários e serviços de uma organização. A tecnologia é implementada para detectar uma ampla variedade de dados confidenciais, como dados e informações pessoais de clientes e funcionários, documentos financeiros e propriedade intelectual. A DLP monitora como esses dados são acessados e usados, evitando vazamentos, exposição acidental e roubo. A DLP ajuda as empresas a reduzir seus riscos de violação de dados e auditar seus arquivos para publicação acidental de informações confidenciais. À medida que o panorama de conformidade se tornou mais rígido e amplo, a DLP tornou-se uma medida de segurança cada vez mais importante para as empresas se protegerem contra violações de dados dispendiosas e atender às demandas da legislação de conformidade.

Por que a DLP legada, sozinha, tornou-se extremamente inadequada

As soluções legadas de DLP são usadas para segurança de dados há mais de dez anos. No entanto, com o tempo, esta antiga DLP ganhou a reputação de ser complexa de implementar e gerenciar, cara, limitada em escopo, cada vez menos precisa e inadequada em fornecer o alcance abrangente necessário para o mundo atual de trabalho remoto. As soluções de DLP foram projetadas para proteger dados dentro de um data center e instalações corporativas. Essas soluções têm tentado se adaptar às mudanças trazidas pela era da nuvem. A DLP legada é boa para o que foi projetada, mas agora espera-se que ela cumpra uma função para a qual nunca foi criada: proteger dados na nuvem ou mover-se por várias

nuvens. Além disso, seu modelo baseado em perímetro não consegue acompanhar os dados espalhados por vários locais e aplicações.

A desvantagem das DLPs legadas

Os sistemas legados de DLP, feitos de vários componentes de software e hardware, podem ser difíceis de implementar e manter. A configuração pode ser complexa e cara, o que não é ideal para empresas com orçamento apertado ou recursos de TI limitados. Abranger empresas altamente distribuídas também é um desafio importante e caro porque a arquitetura de DLP on-premises provavelmente deve ser replicada em todas as filiais. E mesmo assim, a abordagem não abrange requisitos modernos importantes, como funcionários remotos, nuvem e flexibilidade de BYOD (bring your own device).

As tecnologias de DLP legadas também precisam de atualizações de software demoradas e ajustes contínuos que criam interrupções nos negócios que não podem simplesmente ser ignoradas. Para evitar essas interrupções, as organizações geralmente evitam as atualizações, podendo ficar meses ou anos atrasadas em relação às versões de DLP, o que significa que não estão usando a proteção atual contra os requisitos de dados, a conformidade e os riscos mais recentes.

Deixar de atualizar e corrigir um sistema de DLP pode levar a vários problemas que nenhuma organização deseja, incluindo vulnerabilidades de segurança, violações de dados e proteção inadequada de dados. Isso pode colocar dados confidenciais em perigo e deixar uma organização fora de conformidade com os regulamentos de proteção de dados. Além disso, a complexidade inerente da DLP legada geralmente resulta em práticas de proteção de dados inconsistentes e excessivamente específicas, fazendo uso ineficiente de recursos e tempo.



ATENÇÃO

Para algumas empresas, a interrupção dos negócios causada por seu sistema de DLP legado é considerada tão grave que elas mudam seus sistemas de DLP para o modo “somente monitorar”, o que significa que o sistema observa o que está acontecendo, mas não aplica a política de proteção de dados. Executar sua DLP sem aplicar a política é como ter um cofre, mas deixá-lo destrancado e esperar muito que ninguém saia com seu dinheiro, joias e documentos importantes.

O dilema do falso positivo

Os sistemas legados de DLP não apenas impõem implementações e processos complicados, mas também precisam de muitos recursos e mão de obra humana para monitorá-los e ajustá-los continuamente de forma eficaz. Como mencionado anteriormente neste capítulo, falsos positivos exercem muita pressão sobre as equipes de segurança.

O número de incidentes que devem ser corrigidos manualmente cresceu a um ponto em que a equipe de resposta a incidentes não consegue considerar, muito menos lidar com todos eles. As equipes de resposta a incidentes recebem muitos alertas que não são realmente problemas e não têm contexto para determinar seu nível de risco após o fato. (Basicamente, eles recebem esses alertas muito tarde após a ocorrência de um incidente, então não apenas os alertas não têm contexto, mas as equipes também são solicitadas a descobrir incidentes que aconteceram no passado com informações de funcionários que não conseguem mais se lembrar do incidente em questão). Esses alertas podem chegar a milhares ou centenas de milhares diariamente e surgem de muitas fontes diferentes. Como muita coisa está acontecendo, as equipes de resposta de segurança simplesmente não conseguem ver todos esses alertas; na verdade, elas precisam ignorar muitos apenas para acompanhar.

Um fator de contribuição significativo é que os dados agora residem e se movem dentro e entre muitos lugares fora da rede do data center gerenciado. As soluções de DLP legadas não estão equipadas para lidar com a variedade e a quantidade cada vez maior de dados e a falta de detecção assistida por ML (machine learning) mais recente, casos de uso modernos de compartilhamento de dados e reconhecimento de contexto. Suas políticas estáticas não podem se ajustar efetivamente aos riscos e contextos comerciais em constante mudança, como quem está usando os dados, de que modo, em qual ambiente e instância de aplicação, se exibem um comportamento seguro e o destino final.

Ferramentas de orquestração e automação de segurança cibernética, como UEBA (user and entity behavior analytics), foram adicionadas para ajudar com parte disso, recebendo alertas e solucionando-os mais rapidamente. No entanto, se o sistema de DLP for impreciso, carecer de contexto de negócios e consciência de risco ou tiver muitas lacunas, os modelos UEBA não funcionarão bem.

Para proteger efetivamente dados confidenciais, um sistema de DLP deve ser integrado e automatizado para monitorar e verificar continuamente a identidade de indivíduos e dispositivos autorizados, seu comportamento, sua colaboração e compartilhamento externo de dados, as aplicações que estão usando e seus riscos e muitos outros fatores contextuais. Essa abordagem zero trust (consulte o capítulo 3) permite recomendações precisas de políticas e regras de resposta a incidentes que se adaptam às mudanças nas condições de risco e ao contexto comercial específico no qual os dados estão sendo usados. Essa abordagem protege os dados sem interromper os negócios.

A DLP legada não tem o alcance necessário para a nuvem

Os sistemas legados de DLP foram projetados com um modelo de segurança baseado em perímetro que pressupõe que todos os dados são armazenados na rede corporativa e nos ambientes gerenciados. Esse modelo não é mais suficiente na era da nuvem, quando os dados são armazenados em vários locais na nuvem e acessados por usuários e dispositivos fora da rede corporativa. Além disso, os sistemas legados de DLP não foram projetados para se integrar à ampla variedade de serviços e infraestruturas em nuvem que estão em uso, dificultando ou impossibilitando o fornecimento de proteção abrangente para dados na nuvem.

Muitas empresas hoje tentam adaptar à nuvem seus sistemas legados de DLP adicionando duas soluções de segurança em nuvem — um CASB (cloud access security broker) para tráfego de aplicações em nuvem e um SWG (secure web gateway) para tráfego web de funcionários remotos e filiais. A esperança é que a adição dessas soluções forneça à DLP legada o “olho na nuvem” necessário para estender seus recursos on-premises (locais) existentes para a nuvem e procurar dados confidenciais fora do perímetro do data center.

Infelizmente, essa abordagem tem algumas falhas críticas:

- » **A integração provou ser muito difícil.** Ela envolve redirecionamentos de tráfego de rede que dependem do altamente complexo ICAP (internet content adaptation protocol), um tópico que foge do escopo deste livro.
- » **CASB e SWG, projetados para a nuvem, geralmente possuem recursos limitados de proteção de dados.**
- » **Mesmo quando a integração é alcançada, essa abordagem acaba se mostrando insustentável.** CASBs usam APIs (application programming interfaces) para se conectar a aplicações corporativas em nuvem, como AWS (Amazon Web Services), Box, Google Workspace, Microsoft 365, Microsoft Teams, Salesforce, Slack e Zoom. Garantir que você tenha uma API para cada aplicação de nuvem que um usuário possa utilizar — e manter essas APIs atualizadas — pode ser um pesadelo.
- » **É difícil consolidar políticas de proteção de dados entre sistemas on-premises (locais) e em nuvem.** Por exemplo, CASBs geralmente não podem duplicar as mesmas políticas que as DLPs legadas. Como essas tecnologias não têm as mesmas capacidades, as políticas e os consoles de gerenciamento ficam fragmentados e fora de sincronia.



Consoles de gerenciamento desconexos e políticas de proteção de dados descoordenadas são dois efeitos colaterais comuns da integração de CASB e SWG à DLP legada.

» **A integração de um DLP on-premises (local) por meio de CASB com uma aplicação na nuvem cria um atraso chamado *latência*.**

Mesmo que sua DLP legada descubra uma violação de política de dados na nuvem, pode levar minutos, horas ou mais para montar uma resposta. Pense neste cenário: a violação aconteceu, foi detectada, mas você ainda não interrompeu a tempo (o que significa que seus dados estão comprometidos!).

No final das contas, combinar DLP legada com tecnologias de nuvem é como tentar combinar dois animais diferentes. Um (CASB) é um serviço de nuvem e o outro (DLP legada) é uma implementação on-premises (local) massiva de hardware e software. O resultado é uma solução frágil que é fácil de quebrar, causa muita latência e é muito difícil de otimizar e manter. As soluções legadas de DLP são on-premises. Ponto final.

Um sistema moderno de DLP deve ser capaz de atender aos padrões de segurança na nuvem em constante evolução de forma adaptativa com suas próprias políticas dinâmicas e recursos de avaliação de risco em tempo real, para que as empresas possam manter seus funcionários, clientes e dados seguros.

A solução? Integrar DSPM com a DLP moderna entregue em nuvem. Indo além da proteção extra que o CASB e o SWG oferecem, o DSPM adiciona a descoberta e a classificação automatizadas de dados em repouso na nuvem para ajudar ainda mais a gerenciar riscos em todo o ciclo de vida dos dados, sejam eles estruturados ou não, onde quer que estejam localizados e independentemente de quem (humano ou não) os esteja acessando ou usando.

Segurança de dados unificada para a era da nuvem e da IA

A transformação digital revolucionou a forma como as organizações fornecem atendimento ao cliente e desenvolvem produtos e serviços. Também teve um impacto imenso na forma como os dados são protegidos. Empresas grandes e pequenas dependem fortemente da tecnologia de nuvem para alcançar o crescimento e a capacitação dos negócios, portanto, as estratégias de segurança devem acompanhar essas mudanças. A arquitetura de segurança de dados deve acomodar a crescente força de trabalho híbrida, mudando para uma estratégia de nuvem para

trazer um alcance mais amplo, maior eficiência, escalabilidade, poderosas habilidades de computação e medidas de prevenção de riscos mais eficazes. Com uma arquitetura de segurança de dados reconsiderada, as organizações modernas podem ter sucesso no mundo do trabalho híbrido e preparar suas empresas para o futuro, o que agora inclui o impacto da IA (inteligência artificial). O uso crescente de IA por funcionários adicionou outra camada de preocupações de segurança para qualquer organização quando se trata de vazamento de dados confidenciais. Ter uma solução unificada de segurança de dados em sua organização pode resolver todos esses desafios, mas é uma tarefa enorme. Com os riscos e avanços em constante evolução nas soluções prontas para a nuvem, agora é o momento certo para considerar isso.

Com DSPM e DLP entregues na nuvem, você não tem nada complicado para implementar, apenas um serviço de nuvem para ativar. Você não precisa lidar com um excesso de componentes e softwares que precisa atualizar individualmente e manter manualmente. Não há mais bancos de dados DLP para manter, especialistas em bancos de dados para contratar ou servidores que se tornam obsoletos ou precisam ser substituídos. E não há mais proxies de hardware que precisam ser atualizados.

As plataformas de segurança de dados entregues na nuvem são projetadas para serem facilmente integradas com serviços de segurança, rede, infraestrutura e nuvem, ao mesmo tempo em que reúnem de forma consistente o risco e o contexto organizacional de outros controles. Os algoritmos de vigilância e detecção de dados funcionam melhor na nuvem, onde o acesso a recursos infinitamente escaláveis reduz a carga em sua infraestrutura de computação, mantendo o ritmo com casos de uso mais recentes e seus inúmeros e crescentes agentes de endpoint. Você não está mais limitado por uma infraestrutura on-premises, e seus usuários estão protegidos onde quer que estejam.

Além disso, como uma arquitetura entregue na nuvem não está vinculada à sua infraestrutura e cronograma, sua solução de segurança de dados permanece atualizada, com atualizações em tempo real disponíveis em qualquer lugar. Essa abordagem é uma ferramenta muito mais eficiente e eficaz para proteger os dados valiosos da sua organização.

Destruindo Mitos

Quando se trata de DSPM e DLP entregues na nuvem, não é segredo que o mercado está saturado de chavões, promessas exageradas e jargões tecnológicos — levando as pessoas a se sentirem sobrecarregadas e confusas com as opções. Mas a verdade é que nem todas as soluções de DLP são criadas iguais. Este livro ajuda você a diferenciar fatos de

propaganda ao avaliar suas opções, oferecendo um guia para recursos e funcionalidades importantes em cada um.

Então, vamos dar um passo para trás e começar por desmascarar alguns mitos comuns sobre a proteção de dados fornecida na nuvem para que você possa se livrar da confusão e tomar uma decisão bem informada sob medida para o seu negócio.

Mito: uma DLP nova é a melhor DLP

Realidade: quando se trata de programas de segurança de dados, você não quer deixar nada ao acaso. Você não precisa apenas de recursos suficientes no programa para garantir a segurança, mas também de um fornecedor dedicado e experiente com experiência comprovada em DLP. As soluções legadas podem não ter sido criadas com a tecnologia de nuvem em mente, mas têm lições a ensinar sobre maturidade para a maioria das soluções de DLP fornecidas em nuvem.

A solução de segurança de dados mais confiável passou por um longo período de maturação e desenvolveu novos recursos ao longo do caminho. Se você está pensando em investir em um programa abrangente de segurança de dados, seu fornecedor deve ser capaz de atender a todas as suas necessidades — desde suporte à nuvem até maturidade dos recursos — para máxima segurança dos dados. A solução mais recente do fornecedor não deve ser confundida com a melhor.

Mito: as DLPs legadas eram imprecisas

Realidade: as DLPs legadas foram criadas por fornecedores que investiram uma década ou mais no desenvolvimento de algoritmos e políticas precisos para identificar e impedir a transferência não autorizada de informações confidenciais.

Precisão não é o verdadeiro problema. O verdadeiro problema, como mencionado anteriormente neste capítulo, são os falsos positivos. Falsos positivos podem levar a uma situação perigosa, onde ameaças reais passam despercebidas, dados confidenciais vazam acidentalmente e a equipe procura maneiras de contornar verificações de segurança onerosas. Isso também leva a equipes de resposta a incidentes com alta qualificação (ou seja, caras) que ficam cada vez maiores para lidar com um volume maior de incidentes. O capítulo 2 explora por que os sistemas de DLP devem ser precisos e exatos para manter a confiança.

Mito: o uso de IA generativa não pode ser protegido pelas soluções atuais de segurança de dados

Realidade: o rápido crescimento da IA generativa, apesar de sua relativa novidade, obrigou as organizações a priorizar a segurança de dados confidenciais ao utilizá-la — o que é crucial para capacitar a força de trabalho sem comprometer a segurança. Muitos líderes de segurança, com base em experiências passadas, antecipam a necessidade de integrar mais uma solução de segurança à sua infraestrutura de segurança existente, muitas vezes desconexa.

No entanto, soluções de segurança de dados que estão na vanguarda dos avanços tecnológicos e permanecem adaptáveis às tendências emergentes devem ser capazes de atender aos requisitos de segurança específicos da IA generativa. Isso inclui compatibilidade com várias iterações de IA generativa, como ChatGPT, DeepSeek, Google Gemini, Microsoft Copilot e outros. Selecionar um fornecedor que possa atender proativamente às suas necessidades em constante evolução neste cenário de rápidas mudanças é fundamental.

Mito: a DLP entregue na nuvem é menos capacitada do que a DLP legada

Realidade: atualmente, muitos sistemas de DLP em nuvem usam menos de 100 identificadores de dados (consulte o Capítulo 2) e verificam apenas alguns tipos de arquivo, o que significa que eles quase não detectam nada. A razão para isso é a falta de maturidade na tecnologia. Ao contrário dos sistemas de DLP que foram desenvolvidos e estão em uso há uma década, esses sistemas foram projetados para se concentrar na solução de novos casos de uso específicos, como aplicações específicas na nuvem, e proteger apenas alguns tipos populares de arquivos. Essa falta de foco amplo significa que eles ainda carecem da precisão necessária para equilibrar efetivamente a proteção de dados e as necessidades comerciais, levando a um atrito contínuo entre os dois. A tecnologia de DLP entregue na nuvem deve ser superior à DLP legada devido à sua capacidade de oferecer escala massiva. Com uma escala maior, você seria capaz de resolver falsos positivos e melhorar a precisão.



ATENÇÃO

Quando se trata de segurança de dados, o velho ditado é verdadeiro: “A experiência conta!” Embora novas opções tentadoras possam parecer ótimas no papel ou à primeira vista, as soluções de DLP maduras, especialmente aquelas integradas com DSPM, podem oferecer um nível

mais profundo de segurança e visibilidade, porque foram desenvolvidas e refinadas ao longo do tempo. Fique com um fornecedor consagrado e teste vários sistemas você mesmo para ter total tranquilidade ao proteger seus dados essenciais.

Mito: um pacote de sistemas de segurança de dados é tão bom quanto uma solução unificada de segurança de dados

Realidade: quando se trata de segurança de dados, iniciativas e programas de segurança que tentam agrupar uma variedade de produtos e serviços de DLP separados de diferentes fornecedores podem parecer um progresso lógico. Afinal, os serviços de DLP já podem vir integrados a determinadas aplicações SaaS, serviços de nuvem pública, firewalls e soluções SWG. Mas, mais cedo ou mais tarde, esses programas de segurança de dados multisserviços não serão suficientes. Ao reunir sistemas distintos que não foram desenvolvidos juntos, a solução pode oferecer pouco conhecimento sobre o contexto e os riscos do negócio. Além disso, os profissionais de segurança de dados acabarão lidando com políticas desconexas e vários consoles. De fato, o escopo de cada serviço de DLP integrado geralmente é limitado a ambientes e canais específicos, abrangendo, por exemplo, apenas o tráfego da Web ou pontos de controle específicos, como uma ou algumas aplicações SaaS. Isso deixará seus dados vulneráveis sempre que estiverem expostos.

Para proteger você e sua organização, busque uma solução totalmente integrada que ofereça segurança de dados abrangente para abordar todas as possíveis áreas de risco em serviços de nuvem, locais on-premises, serviços de e-mail e endpoints, e obtenha alcance total em vários tipos de dados e controles.

- » Identificando os desafios que a DLP legada enfrenta
- » Preparando-se para escalar para possíveis mudanças futuras e crescimento
- » Conhecendo as realidades e limitações da DLP baseada em nuvem
- » Compreendendo como o DSPM e a DLP tornam outras ferramentas de segurança mais eficazes

Capítulo 2

Protegendo toda a empresa centrada na nuvem

Por que é importante que os sistemas de proteção de dados de uma organização protejam toda a empresa, incluindo suas aplicações em nuvem? Porque a perda ou acesso não autorizado de dados pode trazer sérias consequências para a organização e seus stakeholders. Essa abordagem pode parecer óbvia, mas, na prática, muitas forças trabalham contra esse objetivo.

Este capítulo explica por que obter proteção completa de dados em toda a empresa é um processo que oferece ganhos rápidos e benefícios estratégicos de longo prazo.

O Desafio que a DLP Enfrenta à Medida que Evolui

Como discutido no capítulo 1, os sistemas de DLP (prevenção de perda de dados) têm se concentrado primeiramente na proteção de dados armazenados *dentro* de um data center corporativo. No entanto, a empresa moderna não está mais limitada a um local físico. O escopo da empresa

agora inclui os vários endpoints que os funcionários usam para se conectar aos recursos corporativos, bem como as milhares de aplicações entregues em nuvem aprovadas e (hein!?) não aprovadas que podem ser usadas nas empresas (veja a figura 2-1).

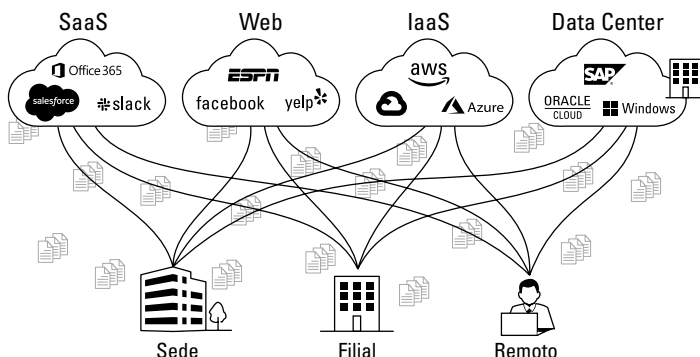


FIGURA 2-1: em uma empresa moderna altamente distribuída, os dados residem e fluem em muitos ambientes novos.

É importante proteger os dados onde quer que estejam, seja na nuvem, em dispositivos remotos, na rede corporativa ou em locais externos. Isso significa que os sistemas legados de DLP, que foram projetados para proteger os dados dentro da empresa, não são mais suficientes.



Embora seja necessário identificar todos os locais onde os dados residem e se movem, ao deslocar o foco da sua proteção de dados para a própria informação, em vez dos locais de origem e armazenamento, você pode obter grandes vantagens em flexibilidade e eficácia. Pense nessa mudança como um time de basquete transitando de uma defesa por zona para uma defesa individual. Ao adotar essa abordagem abrangente, você pode proteger suas informações confidenciais e mantê-las longe de mãos erradas.

Qualquer substituição para um sistema legado de DLP deve fornecer à empresa cobertura completa para canais na nuvem e canais on-premises tradicionais. Mesmo as soluções de DLP mais modernas e entregues na nuvem foram projetadas para abranger apenas canais on-premises (locais) específicos. Elas podem abordar uma rede ou um determinado conjunto de endpoints ou aplicações específicas, mas não abordam toda a variedade de casos de uso modernos.

Para fornecer cobertura corporativa completa, uma solução de DLP deve proteger todas as transmissões de dados estruturados e não

estruturados de e para qualquer local e dispositivo. Isso inclui dispositivos gerenciados e não gerenciados em todos os lugares onde os usuários estão, dentro e fora da rede corporativa, bem como em aplicações SaaS, IaaS (infraestrutura como serviço), e-mail, aplicações privadas e endpoints. Essa abordagem requer uma solução de DLP abrangente e flexível que possa se adaptar às necessidades em constante evolução de uma empresa altamente distribuída.

As seções a seguir examinam as principais considerações ao projetar uma solução de DLP para uma nova empresa sem fronteiras.

Escalabilidade e Preparação para o Futuro

Não muito tempo atrás, o uso de aplicações SaaS era bastante limitado na empresa, mas, com o tempo, o número de aplicações SaaS usadas por funcionários dentro das empresas teve um aumento significativo. Agora, as empresas podem ter centenas de aplicações SaaS aprovadas e (pensamento assustador) os funcionários podem estar usando milhares de aplicações adicionais que a empresa nem conhece.



DICA

Escalabilidade significa não apenas atender às necessidades atuais, mas também se preparar para possíveis mudanças e crescimento futuros. Uma abordagem voltada para o futuro é essencial para criar soluções flexíveis e ágeis capazes de lidar com uma carga de trabalho cada vez maior ou a expansão contínua sem comprometer o desempenho ou a funcionalidade. A escalabilidade ajuda a garantir que seus sistemas permaneçam eficazes e eficientes diante de mudanças imprevisíveis.

Mas a escalabilidade não se trata apenas de abordar novos ambientes e abranger novos locais para onde os dados vão. A escalabilidade também significa lidar com o aumento da velocidade, variedade e volume de dados. A quantidade de dados sendo gerados e coletados hoje não tem precedentes. Com o surgimento de aplicações de colaboração e ferramentas online, os dados agora podem vir na forma de conversas em aplicações como Microsoft Teams, Slack e Zoom, bem como aplicações de e-mail entregues em nuvem, como o Gmail. Também pode ser na forma de imagens, como fotos e capturas de tela. As pessoas são tão propensas a fazer capturas de tela de informações importantes quanto copiá-las e colá-las em um documento. Escalabilidade significa proteger todos os diferentes formatos de dados e todos esses casos de uso, incluindo casos de uso ainda não desenvolvidos.



LEMBRE-SE

A seção “Segurança de dados unificada em ação”, mais adiante neste capítulo, entra em detalhes de como os sistemas de DLP funcionam. Por enquanto, lembre-se de que a funcionalidade básica de um sistema de DLP é detectar dados confidenciais e impedir seu vazamento.

Como a DLP evoluiu de herói para criança problemática

À medida que as organizações adotavam aplicações em nuvem e se expandiam para novos locais, a implantação de sistemas legados de DLP tornou-se cada vez mais incontrolável. Esses sistemas foram projetados para serem instalados e mantidos on-premises, o que significava que precisavam ser duplicados e instalados em cada novo local e filial. Isso acrescentou uma quantidade significativa de complexidade e exigiu muitos recursos, incluindo hardware, manutenção e pessoal. A tendência crescente do trabalho remoto acrescentou mais uma camada de complexidade à medida que os funcionários começaram a acessar dados confidenciais de vários dispositivos e locais diferentes. Tudo isso dificultou o gerenciamento eficaz de seus sistemas de DLP pelas organizações, levando ao aumento de custos e possíveis riscos de segurança.

Você já evitou atualizar seu telefone ou laptop com medo de que isso atrapalhasse um aplicativo favorito ou causasse algum problema irritante? Multiplique isso por milhares e imagine ter que atualizar o software legado de DLP em vários servidores e filiais, bem como em milhares de dispositivos de funcionários. Não é de admirar que alguns clientes se apeguem a versões antigas de seu software de DLP — é muito menos esforço do que tentar uma atualização.



ATENÇÃO

Não realizar atualizações regulares deixa os dados expostos e aumenta os riscos de violações de conformidade e violação de dados.

A DLP precisa funcionar de maneira mais inteligente, não mais difícil

Os sistemas legados de DLP verificam todos os formulários de dados e identificam informações confidenciais a serem protegidas. A ideia é que apenas os dados confidenciais precisam ser protegidos, pois a proteção de dados não confidenciais pode afetar negativamente a produtividade. Por exemplo, embora possa ser importante impedir que certos dados confidenciais sejam compartilhados por e-mail com terceiros, proteger e possivelmente atrasar qualquer comunicação por e-mail com terceiros não é necessário porque isso pode prejudicar a comunicação e a colaboração e produzir muitos alertas para a equipe de resposta a incidentes. Além disso, os funcionários podem ter permissão para usar os

recursos da empresa para atividades não relacionadas ao trabalho, como upload de fotos pessoais nas redes sociais, desde que o conteúdo não seja confidencial e não contenha segredos da empresa. Como os sistemas legados de DLP são feitos de componentes de software e hardware, fazer com que ele verifique todo o tráfego da web e todos os repositórios de arquivos e procure todos os tipos de dados confidenciais requer a implantação de servidores de detecção adicionais, módulos e bancos de dados maiores.

Devido à sua natureza de serem implantados on-premises, os sistemas legados de DLP dependem de recursos de computação de hardware que são necessariamente limitados. Por exemplo, o software de DLP de endpoint instalado nos computadores dos funcionários é projetado com limitações em seus recursos de detecção de dados, como contar com mecanismos básicos de detecção que consomem menos recursos. Isso significa que, embora possam detectar alguns dados confidenciais em endpoints, eles não conseguem usar métodos avançados de detecção, o que pode resultar em quantidades consideráveis de dados confidenciais não detectados. Por exemplo, a DLP legada não pode usar tecnologias avançadas que exigem recursos de processamento substanciais, como ML (aprendizado de máquina) e EDM (correspondência exata de dados; consulte a próxima seção). A DLP entregue na nuvem transfere atividades que demandam muitos recursos para a nuvem, mantendo sua aplicação nos endpoints. A escalabilidade dessa abordagem é uma melhoria drástica, permitindo que a DLP identifique dados como nomes específicos, números de CPF e outros detalhes confidenciais associados a indivíduos.



LEMBRE-SE

A nuvem pode fornecer a escala efetivamente infinita necessária para alimentar esses recursos de detecção, permitindo que os sistemas de DLP se concentrem nos dados mais importantes e os protejam contra acesso não autorizado.

A Necessidade de Precisão

Um mito predominante é que a DLP legada era imprecisa (consulte o capítulo 1). Mas a precisão não é o verdadeiro problema — ou pelo menos não é o principal. O problema principal são os falsos positivos (também discutidos no capítulo 1) principalmente devido à falta de contexto granular. Claro, com os dados se expandindo loucamente em vários dispositivos e aplicações fora das paredes do perímetro de uma organização e os dados confidenciais se tornando mais difíceis de detectar como resultado da explosão de tipos de dados, as DLPs legadas não conseguiram acompanhar e os níveis de precisão diminuíram. Mas o principal

problema é que as soluções legadas de DLP tendiam a ser muito restritivas, sinalizando ações benígnas como violações e até mesmo bloqueando-as, sem entender o contexto de negócios ou o nível de risco. Em um mundo onde a colaboração é fundamental para a nova forma de conduzir os negócios, essas falsas violações se tornaram numerosas e disruptivas.

É importante que a DLP não cause obstáculos para os negócios e nem interrompa o fluxo de dados necessários para práticas comerciais benéficas. Por exemplo, se um funcionário deseja enviar um arquivo para um prestador de serviços confiável que está envolvido em um projeto, você não deseja que a DLP interrompa essa transmissão. De preferência, a DLP deve capacitar as equipes de resposta a serem mais eficazes, amplificando incidentes legítimos de possível perda de dados e filtrando a confusão de falsos positivos.

Exatidão e precisão não eram os principais problemas dos sistemas legados de DLP, mas são para as novas soluções de DLP entregues em nuvem menos maduras. Dois fatores tendem a impactar a precisão e a exatidão desses sistemas:

- » A imprecisão na detecção de dados pode detectar e proteger desnecessariamente muitos dados que não são confidenciais — identificar muitos dados como confidenciais quando não são! — e possivelmente interromper comunicações comerciais legítimas.
- » A falta de métodos de detecção para identificar dados confidenciais — basicamente, dados confidenciais ausentes — pode fazer com que certos formatos de arquivo ou tipos de dados sejam ignorados, como imagens ou formatos compactados, números de passaporte, informações de saúde, números de roteamento internacional e identidades nacionais específicas de cada país, porque o sistema não tem a capacidade de identificar esses tipos de dados e formatos de arquivo.



LEMBRE-SE

Para manter a confiança, os sistemas de DLP devem ser precisos e exatos, rastreando apenas dados confidenciais, sinalizando e bloqueando apenas transferências de dados realmente maliciosas e gerando o mínimo de falsos positivos. Tal sistema requer vários ingredientes principais, conforme descrito nas seções a seguir.

Descoberta e classificação

Os recursos abrangentes de descoberta e classificação de dados em um produto confiável de gerenciamento de postura de segurança de dados (DSPM) localizarão, marcarão e examinarão continuamente fontes de dados estruturadas e não estruturadas em ambientes locais, na nuvem e

híbridos, fornecendo visibilidade completa sobre dados sensíveis e classificação automatizada para apoiar a conformidade regulatória. A descoberta e a classificação também desempenham papéis importantes na minimização de falsos positivos.

identificadores de dados

Identificadores de dados são usados para encontrar informações confidenciais, como números de CPF e números de cartão de crédito, com base em conteúdo descrito genericamente, como expressões regulares (conhecidas como *regex*), uma ferramenta poderosa que ajuda a DLP a identificar automaticamente tipos de dados específicos usando termos, expressões e padrões naturais e cotidianos (“pesquisar um número de nove dígitos”). Uma resposta possível é que o número é um CPF, mas como ter certeza?

Os identificadores de dados buscam a resposta usando regras especiais baseadas no número de dígitos numéricos, padrões de texto, sequências, separações e palavras-chave de proximidade (como número de CPF [SSN], senha [pwd], número de cartão de crédito [CCN] etc.) para reconhecer esses números e mantê-los seguros.



DICA

Aqui estão alguns pontos importantes a serem lembrados em relação aos identificadores de dados:

- » Milhares de identificadores de dados predefinidos e a capacidade de personalizá-los para atender ao seu negócio são necessários para manter suas informações seguras e atender às regras de governança. Além disso, a capacidade de editar ou criar identificadores de dados personalizados é fundamental — cada organização pode ter diferentes informações confidenciais que precisam ser protegidas.
- » Os identificadores de dados devem suportar milhares de tipos de arquivo (DOC, XLS, JPG, PNG, PDF, CSV, ZIP, RAR e assim por diante), formatos e categorias (imagem, análise, arquivo e compactado, planilha, áudio, vídeo, banco de dados e assim por diante) (consulte o capítulo 1).
- » Você deve ter suporte para uma ampla gama de números de identificação específicos de cada país (como informações bancárias internacionais, endereços, códigos postais, identidades nacionais, números de passaporte e códigos de área de telefone) e perfis de conformidade regulatória e de privacidade para garantir que a solução de DLP possa acompanhar os requisitos de governança mais recentes.



DICA

Para que seu sistema de DLP seja eficaz, ele precisa de milhares de identificadores de dados. Isso permite identificar e sinalizar com precisão informações potencialmente confidenciais em estados, regiões e países, independentemente de onde estejam localizadas.

Correspondência exata de dados

EDM é uma maneira de encontrar informações estruturadas específicas de fontes como planilhas e bancos de dados. A EDM permite que uma solução de DLP crie impressões digitais e indexe registros confidenciais de clientes e funcionários, que podem ser usados para identificar um indivíduo usando seu nome completo, CPF, endereço e outros números de identificação. A EDM também pode ser usada para encontrar registros financeiros que identificam os ativos de um indivíduo, como números de cartão de crédito ou números de contas bancárias. Ela pode até ser usada para informações de assistência médica e identificação de produtos e bancos de dados de preços. Com a EDM, uma solução de DLP pode indexar essas informações e localizá-las em qualquer lugar. Para que a EDM seja eficaz e precisa, ela deve corresponder a várias partes de dados indexados e combinar campos de dados a partir de um registro específico. Ela também deve ser capaz de indexar bilhões de registros para dar suporte a organizações em crescimento, seus bancos de dados em expansão e a quantidade cada vez maior de informações nos tempos atuais. Portanto, a escala de processamento é importante para a EDM.

Recursos avançados de detecção de dados

Com mais tipos de dados e formas de transferi-los do que nunca, as organizações precisam que seu sistema de DLP seja capaz de detectar informações confidenciais com precisão. *Recursos avançados de detecção* são um termo genérico que se refere a coisas como:

- » **Reconhecimento óptico de caracteres (OCR) e reconhecimento de imagem baseado em inteligência artificial (IA):** Esses recursos estão se tornando cada vez mais importantes para a segurança de dados. Hoje em dia, as pessoas tiram fotos de documentos, formulários, carteiras de identidade, quadros brancos e até de outras fotos com muita facilidade. Por exemplo, as pessoas costumam fazer capturas de tela ou tirar fotos para capturar informações rapidamente e compartilhá-las com um colega. Usando o OCR, uma solução de DLP pode extrair texto de uma imagem e, em seguida, aplicar a classificação de dados com base nas políticas de detecção existentes.
- » **IA e ML:** A classificação de imagens por IA e ML, usando métodos de detecção sofisticados, pode reconhecer tipos comuns de arquivos

e documentos — como cartões de crédito, formulários fiscais, acordos de confidencialidade (NDAs), formulários sobre fusões e aquisições (M&A) e patentes — sem necessariamente extrair o conteúdo que eles contém. Esses métodos podem detectar partes de conteúdo embaçadas, enrugadas e danificadas, mesmo quando as informações são difíceis de ler com clareza. Isso porque os algoritmos são treinados para identificar padrões e características específicas de cada tipo de documento, como layout, fontes e cores utilizadas. Além disso, eles podem considerar o contexto em que o documento está sendo usado. Isso permite que a IA classifique o documento com precisão, mesmo em condições desafiadoras, como imagens de baixa qualidade ou documentos danificados.

» **Impressão digital de arquivos e documentos:** essa é uma técnica essencial para as organizações garantirem a segurança e a confidencialidade de seus documentos mais importantes e arquivos altamente confidenciais. Ao indexar todo o documento e detectar cópias exatas ou parciais de seu conteúdo, as organizações podem impedir a exfiltração e a duplicação não autorizadas de suas informações confidenciais (como documentos de fusões e aquisições, informações de pré-lançamento, projetos de engenharia ou dados relacionados a investidores). Essa técnica é especialmente útil na detecção de cópias de arquivos confidenciais em ambientes de risco e canais de transmissão, como e-mails enviados e uploads para instâncias de aplicações pessoais.

As soluções legadas de DLP realmente forneciam algumas respostas no passado apenas on-premises, mas não conseguem mais acompanhar. Elas simplesmente não têm poder de computação ou escalabilidade suficientes.

Muito contexto e um modelo de proteção de dados zero trust

Assim como as ondas do oceano estão mudando e se movendo constantemente, o mesmo acontece com as pessoas, redes, aplicações, dados e regras de governança dentro de uma empresa. Para ficar à frente dos riscos potenciais, um sistema de DLP e a estratégia relacionada devem ser capazes de se adaptar e responder com rapidez e eficácia ao cenário de dados em constante mudança. Essa agilidade (também conhecida como *entender o contexto*) permite que o sistema de DLP proteja efetivamente os dados confidenciais, minimize os riscos de violação de dados e garanta a conformidade com os regulamentos relevantes sem afetar a produtividade do usuário e causar conflitos na continuidade dos negócios.

Para alcançar tais nuances e flexibilidade, uma plataforma de proteção de dados fornecida em nuvem deve se integrar à infraestrutura de rede e segurança mais ampla de uma organização. Essa plataforma DLP também deve coletar constantemente informações de várias fontes, como gerenciamento de identidade, análise comportamental, registros de rede, ferramentas de segurança em nuvem, análise de ameaças, segurança de rede, SaaS e posturas de segurança em nuvem, CASB (Corretor de Segurança de Acesso à Nuvem) — índices de confiança na nuvem nativos e posturas de segurança de endpoint. Essas informações de risco e segurança permitem a definição de níveis de acesso apropriados e a imposição de políticas corretas de segurança de dados. Elas conseguem isso observando coisas como quem é a pessoa, onde ela está, o que ela está fazendo, quão seguro é seu dispositivo, se a rede é confiável, a reputação da aplicação que ela está usando, para onde os dados estão sendo transferidos e muito mais.



DICA

Ao estar ciente dos riscos e do contexto, uma plataforma de proteção de dados pode se adaptar continuamente e fornecer alta eficácia e resposta precisa a incidentes.

O capítulo 3 abrange o conceito zero trust e seu papel central em uma DLP eficaz. Por enquanto, lembre-se de que zero trust é uma estratégia de segurança essencial que pressupõe que todos os usuários, dispositivos e redes no ambiente de uma organização são potencialmente mal-intencionados e devem ser tratados com suspeita a qualquer momento.

Zero trust significa que todo acesso a recursos e sistemas é estritamente controlado e verificado, independentemente de o usuário ou dispositivo estar dentro ou fora do perímetro da rede. O contexto é o mecanismo que alimenta uma estratégia zero trust permitindo que o sistema de DLP faça escolhas bem informadas sobre quando permitir ou proibir a ocorrência de atividades relacionadas a dados.



LEMBRE-SE

Trabalhar com soluções integradas de segurança e tecnologias de proteção de dados adjacentes é o que diferencia uma *ferramenta* de proteção de dados de uma verdadeira *plataforma* de proteção de dados.

Segurança de dados unificada em ação

A DLP está no centro da estrutura de segurança da informação de uma empresa e ajuda a tornar outras ferramentas de segurança mais eficazes. Ela executa várias funções básicas, incluindo as seguintes:

- » **Identificar e monitorar dados confidenciais onde quer que eles estejam e se movam, como:**

- *Dados em movimento*, que são dados que cruzam a internet, redes, aplicações e dispositivos (como uploads e downloads).
- *Dados em repouso*, que são dados que estão armazenados. Isso pode ser qualquer coisa, desde o armazenamento em suas aplicações privadas até um aplicação SaaS adotada pela empresa, como quando os dados do cliente são colocados no Salesforce ou documentos com somente uso interno armazenados e compartilhados no Microsoft OneDrive ou no Microsoft SharePoint.
- *Dados em uso*, que são dados que estão sendo acessados, processados ou manipulados ativamente, como transferência para USB, impressão, comunicação por e-mail ou dados enviados por fax. (As pessoas ainda enviam fax?!)

» **Monitorar o ambiente de dados para detectar quem está acessando os dados e o que eles estão fazendo com esses dados:**

Ao monitorar as ações, a DLP pode detectar incidentes, como compartilhamento não autorizado de informações confidenciais, que podem violar a política corporativa, e tomar medidas para resolvê-los. Isso ajuda a garantir que dados confidenciais não sejam acessados ou usados sem os privilégios corretos (funcionários versus estranhos, ou empresa versus dispositivo pessoal) ou autorização ou moderação (como downloads em massa suspeitos de grandes quantidades de arquivos) e que quaisquer possíveis violações de segurança sejam rapidamente identificadas e resolvidas.

» **Executar ações automaticamente para impor políticas, por exemplo, interrompendo o fluxo de dados, criptografando os dados, colocando em quarentena as informações confidenciais ou não compartilhando os dados em uma aplicação SaaS:**

Por exemplo, se um funcionário usar o OneDrive para compartilhar intencionalmente ou acidentalmente um arquivo contendo informações confidenciais com usuários externos, a DLP pode cancelar o compartilhamento do arquivo automaticamente para impedir a divulgação não autorizada das informações.

» **Fornecer treinamento aos usuários notificando-os automaticamente sobre violações e os motivos por trás delas, e ao mesmo tempo instruí-los sobre práticas seguras de manipulação de dados:**

A notificação também ajuda a instruir instantaneamente os usuários sobre as políticas de segurança, reduzindo a necessidade de equipes de resposta a incidentes para triagem manual de problemas. Uma DLP moderna também deve ser capaz de notificar os usuários instantaneamente, e encaminhar as notificações aos gerentes, à equipe de resposta ou ao RH, conforme necessário.

Agora É a Hora de Mudar Sua DLP

A DLP legada tem sido uma solução de segurança confiável há anos, e não é de admirar que tantos profissionais ainda sejam fãs. Afinal, como observado anteriormente, esses sistemas passaram por intenso desenvolvimento na última década para proteger redes locais contra ameaças na era pré-nuvem.

Os fornecedores de DLP legada tentaram preencher a lacuna entre seus sistemas e os requisitos comerciais modernos baseados na nuvem usando tecnologias como SWGs (gateways de segurança web) entregues na nuvem e soluções CASB, usando a integração do ICAP (Protocolo de Adaptação de Conteúdo da Internet).



ATENÇÃO

Infelizmente, a maioria dos sistemas legados de DLP não são projetados para lidar com casos de uso de nuvem e trabalho híbrido, que exigem integrações e recursos com serviços em nuvem que os sistemas legados de DLP não suportam prontamente. Isso pode resultar em problemas de compatibilidade e baixo desempenho.

Todas essas e outras limitações discutidas no capítulo 1 tornaram a DLP legada impopular, levando muitas organizações a simplesmente desativar essas ferramentas. À medida que as organizações movem cada vez mais seus dados para a nuvem, elas têm uma necessidade crescente de sistemas de DLP entregues em nuvem que possam reconhecer os contextos mutáveis e os riscos associados ao gerenciamento de dados. Esses sistemas devem ser fáceis de implantar, expandir e dimensionar, abrangendo casos de uso legados e modernos. Por serem entregues em nuvem, eles também estão sempre atualizados, fornecendo proteção aprimorada à medida que o contexto de negócios e os riscos evoluem.

NESTE CAPÍTULO

- » Entendendo como a segurança de dados desatualizada pode prejudicar seus negócios
- » Descobrimos tipos de contexto de dados e mantendo as atividades comerciais em andamento
- » Adaptando-se às mudanças nas condições de risco para proteger seus dados
- » Garantindo que os casos de uso empresariais modernos possam ocorrer com segurança
- » Avaliando o contexto do negócio, os riscos e comportamento do usuário para manter seus dados seguros no futuro

Capítulo 3

O papel do zero trust na segurança de dados unificada

Um conceito muito importante na segurança atual — tanto em DLP (prevenção contra perda de dados) quanto em outras áreas — é o zero trust. Uma estratégia zero trust assume que todos os usuários e dispositivos, mesmo aqueles dentro da rede da organização, podem ser prejudiciais e não confiáveis. Isso significa que o acesso a dados e sistemas confidenciais não é concedido automaticamente com base na identificação pessoal e na afiliação organizacional. O acesso é dado após cuidadosa autenticação, verificação das posturas de segurança e consideração do contexto de risco, que é continuamente reavaliado. O zero trust não deve prejudicar a produtividade — ele deve permitir o uso seguro de dados confidenciais e oferecer suporte a práticas empresariais modernas com segurança em mente, adaptando-se automaticamente às mudanças nas condições de risco.

O zero trust avalia continuamente a confiabilidade de cada indivíduo ou dispositivo e ambiente operacional antes de conceder acesso a dados confidenciais ou a determinados usos desses dados confidenciais.

Mesmo que alguém seja um funcionário e tenha recebido acesso antes, ele ainda precisa ser avaliado com cuidado (por exemplo, com verificação de identidade, verificação de dispositivo e conexão de rede, avaliação dos riscos das aplicações que está acessando, e seu comportamento precisa ser monitorado para garantir que ele *permaneça* confiável). Se ele começar a se comportar de forma suspeita ou mostrar sinais de negligência, como compartilhamento excessivo de dados, o sistema enfrenta suas ações, por exemplo, reduzindo seus privilégios. Isso ajuda a proteger dados confidenciais contra possíveis riscos de perda de dados e garante que apenas indivíduos confiáveis possam acessá-los e compartilhá-los com outros indivíduos confiáveis.

Este capítulo explora os benefícios de uma abordagem zero trust e o papel fundamental que ela desempenha em um ambiente de segurança de dados unificada.

Os Riscos da Segurança Desatualizada

Os sistemas de DLP foram criados para ajudar a evitar que informações confidenciais saiam de uma empresa. As versões legadas abordam um número limitado de cenários comuns de perda de dados; seu principal objetivo é identificar dados confidenciais e mantê-los dentro da organização, usando uma abordagem baseada em perímetro focada no controle do fluxo de dados dentro e fora da rede da organização.

Usando uma abordagem chamada *confiança implícita*, a DLP legada se concentra na detecção e resposta a violações de dados predefinidas. Mas essa abordagem carece de contexto sobre os usuários e seus motivos de negócios e os riscos associados de uma ação específica.

Por exemplo, um sistema legado de DLP pode pesquisar números de CPF e bloquear qualquer tentativa de enviar um número de CPF para fora do perímetro da empresa. Em outro caso, ele pode impedir que dados confidenciais sejam enviados para uma aplicação SaaS (software como serviço) sem distinguir entre uma instância corporativa de uma aplicação SaaS aprovada como o Microsoft Teams e uma instância pessoal dessa mesma aplicação. Essa abordagem pode parecer segura, mas na verdade é bastante rígida e carece de informações sobre usuários, dispositivos, redes, aplicações e destinos que possam revelar atividades sancionadas. A confiança implícita é um inibidor de negócios que impede a comunicação aberta e o fluxo de dados necessários para o crescimento de um negócio moderno.



ATENÇÃO

Como ela não reconsidera continuamente o contexto e os riscos dos negócios, um sistema de DLP legado não pode tomar decisões informadas sobre proteção de dados e pode causar interrupções desnecessárias nas operações comerciais.

Com políticas flexíveis, a confiança implícita concede acesso a dados confidenciais sem verificar continuamente a identidade e a confiabilidade do usuário ou dispositivo. Isso é problemático porque deixa a organização vulnerável ao possível manuseio incorreto de seus dados confidenciais. Depois que os dados confidenciais deixam o perímetro, eles ficam fora do controle da segurança da organização.

Essa situação é um grande problema na era da nuvem. Dados confidenciais são usados e compartilhados fora das fronteiras da empresa até mesmo para as funções comerciais mais rotineiras. Por exemplo, aplicações e serviços em nuvem comuns, como Dropbox e Google Drive, permitem que os funcionários acessem, compartilhem e colaborem usando dados confidenciais dentro e fora dos ambientes corporativos. Mas os sistemas legados de DLP que usam confiança implícita interromperiam uma colaboração legítima ou permitiriam que os dados vazassem para o mundo externo, tornando-os vulneráveis a possíveis ameaças.

A proteção de dados zero trust permite o uso e compartilhamento de dados confidenciais, desde que as condições de segurança sejam continuamente verificadas. Ela permite que dados confidenciais fluam e sejam compartilhados entre usuários e dispositivos e armazenados em diferentes serviços de nuvem porque verifica continuamente as condições de segurança, como identidade do usuário, dispositivo, rede e segurança de aplicação e o comportamento do usuário ao longo do tempo. A proteção de dados zero trust se aplica especificamente a dados confidenciais e garante que todas as condições de segurança sejam atendidas o tempo todo, permitindo trabalho híbrido, nuvem e casos modernos de uso empresarial.



LEMBRE-SE

Um sistema de segurança de dados unificada que usa princípios zero trust monitora e controla dados em qualquer lugar que os usuários corporativos desejem se conectar e acessar dados, e em qualquer lugar que os dados possam ser armazenados e transferidos em repositórios de aplicações em nuvem e ambientes on-premises (locais).

Outro problema com as abordagens de segurança tradicionais baseadas em vários produtos e confiança implícita é que elas são muito isoladas, aplicando apenas um controle de segurança por vez sem integrar todos os controles de segurança e sem compartilhar inteligência de risco. Isso significa que diferentes controles de segurança são isolados e não integrados em uma plataforma de segurança coesa, deixando lacunas em sua estratégia geral de segurança. Para proteger totalmente seus dados, você precisa de vários controles de segurança trabalhando juntos e compartilhando inteligência.

A abordagem zero trust adota uma visão mais holística e dinâmica para a proteção de dados. Ela considera o contexto do usuário, dispositivo,

rede e outros fatores para tomar decisões mais informadas sobre proteção de dados. Essa abordagem oferece suporte à integração da DLP com outros controles de segurança e ferramentas de produtividade e pode monitorar e adaptar-se continuamente às mudanças de ameaças, riscos e condições de negócios.

No geral, as organizações que usam DLP com base na confiança implícita devem confiar na falsa suposição de que os usuários dentro de uma organização são confiáveis, são cuidadosos com a segurança e nunca comprometerão dados confidenciais. Na verdade, devido à falta de contexto de segurança, uma aplicação restritiva de políticas de DLP geralmente causaria a interrupção de processos de negócios legítimos. Por outro lado, a DLP baseada em zero trust monitora e controla de perto como os dados são usados o tempo todo para evitar violações de políticas de dados de forma adaptativa.

Um sistema de DLP baseado em confiança implícita protegeria um número de cartão de crédito permitindo que usuários autorizados acessassem dados confidenciais enquanto negaria acesso a usuários não autorizados. Isso pressupõe que os usuários autorizados podem ser confiáveis para lidar com os dados com segurança e não usá-los indevidamente.

Em contraste com os sistemas legados de DLP baseados em confiança implícita, um sistema de DLP baseado em princípios zero trust não depende da suposição de confiança entre os usuários. Em vez disso, ele protege dados confidenciais, como números de cartão de crédito, exigindo que todos os usuários passem por um processo de autenticação antes de acessar esses dados, independentemente de seu nível de autorização. Isso pode incluir MFA autenticação multifator), como uma senha e um código único enviado a um dispositivo móvel.

O sistema também avalia continuamente os riscos potenciais de dispositivos, usuários, dados e aplicações. Ele verifica se os dispositivos são confiáveis e protegidos, se as aplicações e suas instâncias (ou seja, corporativas versus pessoais) usadas são seguras e compatíveis, se a rede é segura e confiável, se os dados são compartilhados com destinos e destinatários confiáveis e se o comportamento do usuário é compatível. Essas condições são continuamente verificadas e o sistema adapta sua resposta de proteção de acordo. Além disso, o sistema monitora e rastreia o acesso do usuário a dados confidenciais, alertando os administradores sobre qualquer comportamento suspeito ou possíveis violações e treinando os usuários sobre práticas seguras de uso de dados em caso de violação das políticas corporativas. Essa abordagem reduz o risco de acesso não autorizado a dados confidenciais porque o sistema verifica todos os usuários antes de conceder acesso e minimiza os riscos

para dados confidenciais ao longo do tempo instruindo os usuários em tempo real.

O Contexto Permite que Sua DLP Diga Sim a Atividades Comerciais Importantes

O zero trust ajuda os sistemas de proteção de dados a tomar decisões bem informadas sobre permitir ou restringir determinadas atividades. Ele faz isso considerando vários fatores ou contextos, como a identidade do usuário, o dispositivo usado, a confiabilidade da aplicação e o contexto dos dados envolvidos. (O zero trust reúne o contexto com a ajuda de outras soluções, discutidos mais adiante na seção “A DLP Não Deve Ficar Sozinha”.) Ao levar em consideração todos esses contextos, aplicar os princípios zero trust pode determinar com mais precisão se uma determinada atividade é benéfica e necessária para o negócio e pode dizer sim a ela. Isso ajuda a garantir que os dados sejam protegidos e o risco de violações de segurança ou outras ameaças seja minimizado, permitindo que as operações empresariais continuem funcionando sem problemas.

A lista a seguir define os tipos de contexto usados no zero trust:

- » **Contexto do usuário:** quem está fazendo uma ação ou quem é o destinatário de uma ação. Essas informações ajudam a determinar se o comportamento de um usuário representa um risco para dados confidenciais. Por exemplo, suponha que um usuário de repente esteja movendo muito mais dados do que o normal, fazendo login de lugares estranhos ou agindo de maneira estranha em comparação com antes. Isso pode ser um sinal de comportamento arriscado ou malicioso. O mesmo se aplica se um usuário estiver acessando ou usando dados confidenciais e/ou enviando-os para aplicativos pessoais. Com base em sua identidade e comportamento, você pode alterar os privilégios de um usuário para garantir que os dados confidenciais sejam protegidos e apenas usuários autorizados possam acessar esses dados para compartilhá-los com destinatários autorizados e transferi-los para destinos seguros.
- » **Contexto do dispositivo:** o dispositivo que está tentando acessar seus dados. Você precisa considerar se o dispositivo é pessoal ou corporativo, a postura de segurança dele e se possui as últimas correções e atualizações. Você também pode observar fatores próximos ao dispositivo, como a confiabilidade do local de onde ele está se conectando. Considerando todos esses detalhes, você pode determinar o nível certo de privilégios para o dispositivo com base em quão confiável e arriscado ele é. Mesmo que um usuário geralmente seja

confiável, seu dispositivo ainda pode estar comprometido ou representar um risco de segurança, portanto, o contexto do dispositivo é fundamental para determinar os privilégios que você deve conceder.

- » **Contexto da aplicação:** a reputação e a confiabilidade do aplicativo usado para acessar ou manipular dados. Isso é importante porque, se uma aplicação tiver má reputação ou não for confiável, poderá representar um risco à segurança dos dados acessados ou manipulados. Os sistemas de proteção de dados podem depender de outros sistemas, como um agente de segurança de acesso à nuvem (CASB) para coletar informações sobre os atributos relacionados à conformidade e ao risco do aplicativo. Essa informação pode ajudar o sistema a determinar se a aplicação representa um risco, como violar o RGPD (Regulamento Geral de Proteção de Dados) da União Europeia ao potencialmente expor dados confidenciais excessivamente.

Um usuário pode ter acesso a várias instâncias de uma aplicação em nuvem, o que requer um controle mais granular sobre dados confidenciais para evitar o compartilhamento acidental com contas pessoais. Aplicações de comunicação colaborativa como o Microsoft Teams e o Slack também podem representar um risco se os canais dessas aplicações tiverem usuários corporativos e externos, portanto, o sistema deve ser capaz de diferenciá-los para evitar vazamentos de dados. Lembre-se de tudo isso para garantir que os aplicativos que você está usando sejam conceituados e confiáveis e para proteger seus dados de possíveis riscos.

- » **Contexto dos dados:** o quanto é confidencial um dado específico, assim como seu formato, tamanho e outros fatores. O contexto dos dados também inclui onde os dados estão sendo usados e se esse uso é legítimo. Saber o tipo de dados que estão sendo acessados ou movidos e se eles pertencem ao local onde estão sendo usados ajuda a identificar atividades potencialmente arriscadas. Dados confidenciais sendo acessados ou transferidos para um local não autorizado requerem ação para evitar vazamento ou violação de dados. O contexto dos dados é crucial para garantir que os dados sejam tratados adequadamente e acessados apenas por usuários autorizados em locais autorizados com base em seu nível de importância. Ele ajuda a determinar se uma atividade é necessária para o negócio e se vale a pena correr o risco.



ATENÇÃO

A maioria das soluções de DLP, não apenas a DLP legada, causa problemas na forma como sua empresa funciona porque normalmente não coleta informações suficientes sobre o negócio e os riscos envolvidos. A maioria das soluções DLP força a organização a depender de equipes de resposta a incidentes para tomar decisões manuais sobre o que fazer. Isso é frustrante, ineficiente e caro!

Com o zero trust, esses problemas certamente são minimizados. Um sistema de segurança de dados unificada baseado em princípios zero trust considera todos os riscos de itens como usuários, dispositivos, dados, redes e aplicações. Dessa forma, o sistema tem uma compreensão muito melhor dos riscos envolvidos e pode tomar automaticamente as decisões corretas sobre a proteção de seus dados com base em políticas dinâmicas de proteção de dados adaptadas às suas necessidades específicas de negócios. O zero trust ajuda você a manter seus dados seguros e seus negócios funcionando sem problemas.

A DLP Não Deve Ficar Sozinha

Os controles de dados são usados em sistemas legados e novos de DLP. A DLP é, de fato, projetada para identificar dados confidenciais e protegê-los. O problema com a maioria desses controles de dados é que eles não têm contexto. A DLP precisa fazer parte de uma plataforma maior, baseada em princípios zero trust, que usa todo o contexto disponível para tomar decisões informadas. A DLP precisa de ajuda e inteligência de outras soluções, como DSPM (Gerenciamento de Postura de Segurança de Dados), para reunir todo o contexto necessário, como contexto do usuário, contexto do dispositivo, contexto da aplicação e contexto dos dados. É por isso que um sistema baseado em zero trust é integrado e se concentra em controles de dados contextuais em vez de apenas confiar cegamente em tudo. É uma forma de se adaptar às mudanças nas condições de risco e proteger automaticamente seus dados sempre com a resposta mais adequada.



DICA

Na proteção de dados zero trust, procure controles consolidados em que cada controle compartilhe informações e trabalhe em conjunto para proteger seus dados. Por exemplo, o Netskope Intelligent Security Service Edge (SSE) habilita diretamente o zero trust e permite o compartilhamento e o contexto entre os controles — incluindo a DLP em seu centro — tornando super fácil e eficiente proteger seus dados.

O Netskope Intelligent SSE suporta sua plataforma de DLP abrangente com várias outras soluções de segurança. Algumas das mais importantes são:

» **SWG (gateway de segurança da web):** um SWG é uma solução de segurança que fica entre os usuários e a internet, garantindo conexões seguras com a web e protegendo contra ameaças baseadas na web. O Netskope DLP via SWG garante que dados confidenciais não vazem através de tráfego da web não confiável e arriscado, incluindo tráfego criptografado. Ele detecta, monitora e protege dados corporativos confidenciais de vazamentos e exposição em todas as conexões

da web, incluindo escritórios domésticos, filiais e locais de Wi-Fi público.

- » **CASB:** o Netskope DLP por meio do CASB descobre, monitora e protege dados confidenciais em aplicações SaaS, IaaS (infraestrutura como serviço), redes corporativas e filiais, força de trabalho móvel, serviços de e-mail e endpoints de funcionários. Este serviço centralizado entregue na nuvem impõe políticas unificadas de proteção de dados em todos os lugares em que dados confidenciais são armazenados, usados ou transferidos e abrange dados confidenciais em movimento e em repouso. Ele abrange milhares de aplicações SaaS e tem conhecimento exclusivo dos dados transmitidos para instâncias de aplicações pessoais (por exemplo, OneDrive corporativo para OneDrive pessoal) e aplicações arriscadas. Ele verifica milhares de tipos de arquivos diferentes, bem como postagens e comunicações assíncronas por meio de aplicativos de colaboração e serviços de e-mail. As políticas de proteção de dados, conformidade e privacidade de dados são aplicadas de forma consistente em serviços de nuvem pública e sincronizadas automaticamente em toda a plataforma de DLP.
- » **DSPM:** o Netskope One DSPM automatiza a identificação de todos os dados que sua organização possui, onde esses dados estão localizados, quem tem acesso a eles e os riscos que as interações com eles representam. Ele também automatiza a descoberta e a classificação abrangentes de dados, além de localizar, marcar e verificar continuamente fontes de dados estruturados e não estruturados em ambientes on-premises (locais), na nuvem e híbridos. Isso fornece visibilidade completa de dados confidenciais e classificação automatizada para dar suporte à conformidade regulatória.
- » **SSPM (Gerenciamento de Postura de Segurança de SaaS) e CSPM (Gerenciamento de Postura de Segurança na Nuvem):** essas tecnologias fornecem gerenciamento de postura para SaaS e ambientes de nuvem pública para garantir segurança e conformidade. Elas monitoram e avaliam continuamente a postura de segurança, identificando possíveis riscos e configurações incorretas e fornecendo informações e recomendações utilizáveis. Os recursos de correção automatizada abordam os problemas identificados em tempo real.
- » **Software de proteção de endpoint:** Netskope Endpoint DLP é uma solução que detecta, monitora e protege dados confidenciais em endpoints de funcionários. Como a solução é integrada em um único cliente Netskope, não há necessidade de implantar um agente separado. O Netskope Endpoint DLP minimiza a utilização de recursos enquanto oferece um conjunto completo de recursos, incluindo classificadores baseados em ML (aprendizado de máquina), OCR (reconhecimento óptico de caracteres), impressão digital de arquivos, EDM

(correspondência exata de dados) e muito mais. Utilizar o serviço de DLP entregue na nuvem e a inteligência proveniente de toda a plataforma de DLP ajuda a evitar a verificação duplicada de dados originados na nuvem, resultando em uma experiência de usuário sem obstáculos e resultados de proteção mais fortes.

- » **UEBA (análise de comportamento de usuários e entidades):** esse controle de segurança avalia continuamente o comportamento do usuário para identificar qualquer atividade incomum ou potencialmente arriscada. No passado, UEBA costumava ser um controle de segurança isolado, mas precisava ser integrado à DLP para ser eficaz. Ao ingerir registros de violação de DLP e sinalizar comportamentos de risco para avaliação adicional, o UEBA pode informar alterações subsequentes na aplicação de políticas e ajudar a manter seus dados seguros.
- » **IAM (gerenciamento de identidade e acesso):** IAM é a prática de gerenciar e controlar o acesso a recursos com base na identidade do usuário. Ele inclui tecnologias como MFA (autenticação multifator), SSO (logon único) e ACLs (listas de controle de acesso). A Netskope trabalha junto a muitos fornecedores de IAM para garantir que apenas usuários autorizados possam acessar recursos específicos e se proteger contra acesso não autorizado. IAM é uma parte essencial da estratégia de segurança zero trust de qualquer organização, ajudando a proteger os recursos e garantir a conformidade com as políticas e regulamentações de segurança.
- » **Proteção de e-mail:** a Netskope fornece uma solução de DLP muito extensa para e-mail como Microsoft 365 e Gmail, e para dados em movimento e em repouso. A solução protege e-mails enviados confidenciais em tempo real por meio de proxy SMTP (simple mail transfer protocol) e webmail e pode distinguir dados confidenciais enviados de uma conta de e-mail pessoal versus dados enviados por uma conta de e-mail corporativa ou por serviços de e-mail privados.
- » **Acesso à rede de Confiança Zero (Zero Trust Network Access, ZTNA):** o Netskope DLP fornecido através do Netskope Private Access (NPA), uma solução de acesso remoto, evita a perda e exfiltração de dados em recursos privados no data center e em ambientes de nuvem pública, garantindo proteção de dados para acesso baseado em navegador a aplicações privadas em qualquer lugar de onde os usuários estejam se conectando.

Ao combinar esses componentes essenciais em uma única plataforma integrada, a plataforma SSE da Netskope fornece uma solução de segurança abrangente que pode proteger sua organização e os dados dela de uma ampla gama de ameaças.

Colocando os princípios de confiança zero em prática com a segurança de dados



LEMBRE-SE

O objetivo da proteção de dados zero trust não é apenas impedir que dados confidenciais saiam da empresa. É também permitir que casos modernos de uso comercial aconteçam, mantendo sempre a segurança e o risco em mente.

Isso significa oferecer suporte a usuários em diferentes locais e incentivar a colaboração, mantendo seus dados seguros. A proteção de dados zero trust significa poder trabalhar em qualquer lugar e ainda ter acesso a todos os recursos necessários e colaborar com membros da equipe e parceiros externos sem se preocupar com vazamentos de dados. Usando uma solução unificada como o Netskope SSE, você pode proteger seus dados e aproveitar todos os benefícios dos fluxos de trabalho de dados corporativos modernos.

Aqui estão alguns exemplos de como isso funciona na prática:

- » Imagine que você está trabalhando em seu laptop, conectado à rede da sua empresa usando o Netskope SSE. Você acessa alguns documentos de vendas importantes e começa a trabalhar neles. Mas então você acidentalmente tenta salvar uma cópia dos documentos em sua conta pessoal de armazenamento em nuvem, em vez da instância corporativa da mesma aplicação de armazenamento em nuvem.

Com DLP baseada em princípios zero trust, o sistema reconhece que você está tentando enviar dados confidenciais da empresa para uma instância de aplicação pessoal e impede que os dados sejam salvos. Em vez disso, o sistema exibe uma notificação instrutiva ao usuário, um pop-up que informa imediatamente sobre a violação e lembra o local correto para salvar os documentos. Dessa forma, você pode trabalhar de qualquer lugar e ainda ter acesso a todos os recursos de que precisa sem se preocupar em enviar acidentalmente dados confidenciais para algum lugar ao qual não pertencem. As notificações instrutivas ensinam os usuários sobre práticas seguras e políticas da empresa, minimizando o risco de perda de dados ao longo do tempo e reduzindo a necessidade de longos treinamentos ao longo do ano.

- » Digamos que você esteja colaborando com parceiros externos em um projeto e queira compartilhar alguns documentos com eles. Com DLP baseada em princípios zero trust, o sistema verificará a reputação e a confiabilidade da aplicação que você usa para compartilhar documentos, sua identidade e comportamento, o dispositivo usado e o destino da transmissão.

Se você estiver usando um aplicativo de armazenamento em nuvem pessoal com um nível de segurança diferente do aplicativo corporativo da sua empresa, o sistema pode impedir que você compartilhe os dados por meio desse aplicativo. Em vez disso, ele pode sugerir que você use um aplicativo diferente ou envie os documentos por meio de um canal seguro. A DLP também verificará o destino da transmissão, como, por exemplo, se o destinatário é um usuário externo ou funcionário e se o destino é seguro. A DLP pode enviar uma notificação para você perguntando se você tem certeza sobre o compartilhamento de dados confidenciais com o destinatário externo e pode até pedir que você justifique sua ação. Dessa forma, você pode colaborar com confiança, sabendo que seus dados estão protegidos e somente usuários autorizados podem acessá-los.

Zero Trust Adaptável

O zero trust adaptável significa primordialmente reconhecer que as coisas mudam com o tempo. Isso significa que a proteção de dados zero trust precisa avaliar continuamente o contexto de negócios, o risco e o comportamento do usuário para manter seus dados seguros.

Para visualizar essa situação, imagine um segurança em uma casa noturna. Uma noite, ele está parado na porta quando um grupo de pessoas se aproxima. O segurança verifica as identidades deles e tudo parece certo, então eles deixam o grupo entrar. Mas, à medida que a noite avança, o segurança começa a notar um comportamento estranho em uma das pessoas do grupo. Talvez esteja agindo de forma agressiva ou tentando acessar áreas do clube que não deveria. Com zero trust adaptável, o segurança reconheceria essa mudança de comportamento e tomaria medidas para proteger as outras pessoas e o estabelecimento. Ele pode ficar de olho em determinadas pessoas para garantir que elas não causem problemas ou até mesmo pedir que um indivíduo saia. Dessa forma, o segurança pode manter outras pessoas e o estabelecimento seguros e protegidos, mesmo que o comportamento de alguém mude.

Considere estes cenários comuns que sua empresa provavelmente enfrentará:

- » **O comportamento de alguém muda.** Você tem um funcionário de confiança que sempre teve acesso a determinados dados confidenciais da empresa. Um dia, talvez depois de uma avaliação de desempenho, ele começa a se comportar de maneira diferente. Ele começa a acessar e baixar mais dados confidenciais do que o normal ou a fazer login de locais incomuns. Com o zero trust adaptativo, o sistema

reconhece essa mudança de comportamento e ajusta os privilégios do funcionário de acordo. Por exemplo, o sistema pode restringir o acesso a dados específicos ou notificar a equipe de segurança para uma avaliação mais detalhada. Dessa forma, você pode proteger os dados mesmo que o comportamento de um funcionário confiável mude.

- » **A reputação e a confiabilidade das aplicações mudam.** As aplicações mudam com o tempo; não apenas sua funcionalidade, mas também sua reputação, suas posturas de segurança e sua confiabilidade podem mudar. Por exemplo, uma aplicação de armazenamento em nuvem que já foi considerada segura pode ter uma nova exposição de vulnerabilidade ou configuração incorreta que afeta sua confiabilidade. Com o zero trust adaptável, a solução avaliará continuamente o nível de risco da aplicação e ajustará os privilégios conforme necessário. Dessa forma, você pode proteger seus dados mesmo que a confiabilidade de um aplicativo mude.
- » **Os dispositivos tornam-se comprometidos.** Os dispositivos podem se tornar mais vulneráveis ou até mesmo comprometidos sem que o usuário perceba. Por exemplo, um notebook que já foi considerado seguro pode ser infectado por um malware ou ter suas configurações de segurança alteradas sem o conhecimento do usuário. Com o zero trust adaptável, o sistema avaliará continuamente a postura de segurança do dispositivo e ajustará os privilégios conforme necessário. Dessa forma, você pode proteger seus dados mesmo se um dispositivo for comprometido.
- » **O fluxo de dados muda.** O fluxo de dados pode mudar devido a mudanças nas regras de conformidade em diferentes níveis. Por exemplo, um fluxo de dados pode ser considerado aceitável, mas se o destino se tornar incompatível ou inseguro, os regulamentos ainda podem exigir que a organização proteja o fluxo de dados. Este é o caso do RGPD, que diz que certos dados privados podem não ter permissão para sair da UE, a menos que haja adequação ou um contrato de transferência válido. Com o zero trust adaptável, o sistema avaliará continuamente os riscos e ajustará os privilégios conforme necessário. Dessa forma, você pode proteger seus dados mesmo que as regras mudem.
- » **O cargo ou status de um usuário muda.** Usuários que pedem demissão e avisam com duas semanas de antecedência ainda podem ter acesso a dados sensíveis durante esse período. Com zero trust adaptável, o sistema avaliará continuamente os riscos envolvidos e ajustará os privilégios conforme necessário. Por exemplo, o sistema pode restringir o acesso do usuário a dados específicos ou notificar a equipe de segurança sobre uma ação que precisa de avaliação mais aprofundada.



DICA

O zero trust adaptável avalia o uso de dados de tantas perspectivas quanto possível, a fim de ajustar os privilégios para proteger os dados confidenciais, a reputação da empresa e apoiar a atividade do negócio.

O zero trust adaptável propicia maior proteção ao mesmo tempo em que torna os dados e as pessoas mais produtivos. Ele dá vida à política de proteção de dados adaptável e dinâmica, avaliando continuamente os riscos e ajustando os privilégios conforme necessário. Essa é uma mudança significativa em relação à abordagem típica dos sistemas de DLP, legados e novos, que dependem de uma abordagem única com base na confiança implícita, levando a muitos falsos positivos e à fadiga da triagem de incidentes. Com uma abordagem tão complicada, a equipe de resposta a incidentes é forçada a avaliar manualmente cada incidente para determinar se foi uma violação real e, em seguida, entrar em contato com o usuário responsável (muitas vezes depois de ele ter esquecido sua ação anterior). A equipe então precisa decifrar todo o fluxo de dados — um processo longo e com grande uso de recursos. O zero trust adaptável fornece um modelo para proteção contínua, tornando muito mais fácil manter seus dados seguros e seus negócios funcionando sem problemas.

Segurança de Dados Zero Trust Adaptável da Netskope

A implementação da segurança de dados zero trust adaptável da Netskope é totalmente voltada para o contexto. Ao monitorar o tráfego entre usuários, dispositivos, aplicações, redes e destinos, a Netskope constrói uma compreensão profunda do que está acontecendo em sua organização. Isso permite que o sistema exerça controle granular sobre o acesso aos dados, permitindo que você proteja seus dados confidenciais sem prejudicar as operações empresariais.

Por exemplo, imagine um usuário tentando acessar dados confidenciais da empresa a partir de um dispositivo pessoal. Com a Netskope, o processo começa com a detecção precisa de dados confidenciais. Além disso, considerando vários fatores contextuais, a resposta a incidentes torna-se mais precisa e eficaz, reduzindo a necessidade de triagem manual e minimizando a pressão sobre as equipes de segurança. O sistema avaliaria a postura de segurança do dispositivo, a identidade do usuário e o comportamento do usuário para determinar se o acesso deve ser concedido.

Outros fatores considerados incluem a conexão e localização da rede, vulnerabilidades potenciais, inteligência de ameaças disponível e muito mais. Os riscos e a reputação associados à aplicação serão considerados

pelo Netskope Cloud Confidence Index (CCI), um banco de dados de mais de 83.000 aplicações em nuvem (que continua crescendo!) que a Netskope avaliou com base em cerca de 50 critérios baseados em risco. Esses critérios medem a aptidão empresarial de um aplicativo, levando em consideração a segurança, a auditabilidade e a continuidade dos negócios.

Se o dispositivo for considerado de risco ou o comportamento do usuário for considerado incomum, o acesso pode ser restrito ou a equipe de segurança pode ser notificada para uma avaliação mais detalhada. Se o dispositivo for seguro e o comportamento do usuário for normal, o acesso pode ser concedido.



DICA

A base da segurança de dados da Netskope é seu SSE, que faz parte da plataforma mais ampla Netskope One Secure Access Service Edge (SASE). Essa solução de segurança convergente nativa de nuvem consolida as tecnologias de segurança vitais definidas anteriormente em uma única plataforma integrada. Ao combinar essas tecnologias em uma única plataforma, a Netskope facilita o gerenciamento de sua segurança a partir de um local central. O Netskope SSE é nativo de nuvem, o que significa que pode ser dimensionado de forma rápida e eficiente para atender às necessidades da sua organização. Ele também foi projetado para ser altamente flexível, para que você possa personalizá-lo para atender às suas necessidades específicas de segurança.

O Netskope SSE foi projetado com o entendimento de que a segurança é mais do que a aplicação de políticas. Também é importante instruir os funcionários e incentivar o comportamento seguro de manipulação de dados. É por isso que a solução preserva a capacidade do usuário de tomar decisões de negócios e ao mesmo tempo manter os dados seguros. Por exemplo, quando ocorre uma violação, o Netskope SSE pode direcionar os funcionários para um treinamento sobre como lidar com dados confidenciais, fazer perguntas para avaliar melhor o contexto ou fornecer orientações sobre dicas e práticas recomendadas para trabalhar com segurança em casa. Ao adotar uma abordagem holística para proteção de dados, a Netskope ajuda você a criar uma cultura de segurança em sua organização.

- » Comparando soluções de segurança de dados unificada e legadas
- » Mantendo a segurança em qualquer lugar que você acessar dados
- » Usando políticas unificadas e controles de acesso
- » Analisando os benefícios e diferenciais do Netskope One Data Security

Capítulo 4

Por que a Netskope para segurança de dados unificada

Os diretores de segurança da informação (CISOs) e as equipes de segurança da informação geralmente enfrentam uma decisão difícil: Devemos manter as soluções maduras, porém complexas e custosas, de Prevenção de Perda de Dados (DLP) legadas, ou optar pelas opções baseadas na nuvem, de fácil implantação, que podem não ter toda a profundidade e abrangência de que precisamos? Você estará preparado para responder a essa pergunta depois de ler este capítulo e aprender sobre os principais benefícios de todas as soluções de segurança de dados baseadas em nuvem:

- » **Elas podem fornecer cobertura abrangente.** Não importa onde seus dados estejam armazenados (on-premises ou na nuvem), onde sejam transferidos ou como sejam acessados, uma solução de segurança de dados entregue em nuvem que inclua DLP integrada e DSPM (Gerenciamento de Postura de Segurança de Dados) pode protegê-los.

- » **Elas podem fornecer cobertura para ambientes de nuvem.**
Por meio de aplicativos de software como serviço (SaaS), serviços de nuvem pública de infraestrutura como serviço (IaaS) e acesso web, não importa de onde seus usuários estejam se conectando na moderna empresa com trabalho híbrido, as soluções de segurança de dados baseadas na nuvem têm você protegido.
- » **Elas eliminam a necessidade de configurar infraestrutura adicional porque podem ser implantadas de forma rápida e fácil como serviços em nuvem.**
- » **Elas protegem seus dados confidenciais sem sobrecarregar sua rede e recursos de endpoint.** Um sistema de segurança de dados entregue na nuvem pode processar todos os algoritmos de verificação e detecção de dados que você precisa, em capacidade máxima.
- » **Elas são mais fáceis de integrar com uma ampla gama de outras ferramentas de segurança.**
- » **Elas oferecem maior visibilidade dos dados que são transferidos e armazenados fora de suas instalações corporativas.**
- » **Elas são mais fáceis de manter e atualizar em tempo real e oferecem a capacidade de escalar com mais rapidez e facilidade do que com modelos mais antigos implantados on-premises (no local).**

Depois de ler este capítulo, você terá uma sólida compreensão de como esses benefícios podem se aplicar à sua organização e estará bem equipado para tomar uma decisão informada sobre qual solução de segurança de dados entregue em nuvem é a mais adequada para sua empresa. Ao longo do caminho, você encontrará informações específicas sobre os diferenciais da plataforma Netskope.

Diferenciando as opções de segurança de dados entregues em nuvem

A segurança de dados unificada precisa ser entregue em nuvem. Quando se trata de DLP, dois tipos estão disponíveis. A solução DLP nativa de nuvem geralmente é incorporada em plataformas IaaS e aplicações SaaS de provedores de serviços em nuvem. As soluções integradas de DLP entregues na nuvem geralmente fazem parte de um serviço ou produto de segurança, como um secure web gateway (SWG), firewall de última geração (NGFW) ou agente de segurança de acesso à nuvem (CASB).

Tipo 1: Netskope One Data Security versus soluções pontuais nativas de nuvem

O Netskope One Data Security oferece várias vantagens em relação a soluções pontuais nativas de nuvem mais limitadas.

Ele inclui recursos de Gerenciamento de Postura de Segurança de Dados (DSPM), portanto, descobre e protege seus dados onde quer que residam e se movam, protege o uso organizacional de inteligência artificial generativa (GenAI), gerencia a postura de segurança de dados, suporta a privacidade e conformidade, reduz a exposição de dados maliciosa e negligente, e responde efetivamente a riscos e ameaças de exfiltração de dados. A consolidação dessas funções em uma única plataforma de um único fornecedor simplifica suas operações e reduz seus custos operacionais.

Uma vantagem importante é sua cobertura mais ampla usando um único mecanismo de política de DLP de nível empresarial, que garante que os dados confidenciais sejam protegidos em uma ampla variedade de formatos, canais de comunicação e ambientes, incluindo aplicações SaaS, serviços IaaS, aplicações privadas, serviços de e-mail, compartilhamento de arquivos e transações na web em qualquer lugar onde seus usuários estejam. Ele também inclui proteção de DLP de endpoint, o que é importante porque ajuda a garantir que todos os seus dados confidenciais sejam protegidos, mesmo em endpoints em locais remotos que podem ou não estar conectados à nuvem por meio de qualquer rede específica. O mecanismo único de política de DLP também reduz significativamente a complexidade em comparação com a necessidade de gerenciar diferentes regras de política de DLP para diferentes canais e diferentes serviços em nuvem.

Além disso, o Netskope One DLP é superior em sua precisão de detecção. Ao verificar todo o espectro de tipos de arquivo e formatos de dados, usando uma ampla variedade de algoritmos de detecção de dados e aprendizado de máquina (ML) para entender uma ampla variedade de informações e documentos e seu contexto específico, é possível identificar e classificar com precisão dados confidenciais, mesmo que esses dados sejam armazenados e transferidos em diferentes estruturas, formatos ou idiomas, ou incorporados em imagens. Isso é importante porque ajuda a garantir que nenhum tipo de dado sensível seja vazado ou exposto acidentalmente e que o sistema produza eventos reais de segurança de dados, em vez de falsos positivos.

Por fim, o Netskope One Data Security possui um contexto zero trust incorporado, o que significa que foi projetado para funcionar em uma estrutura de segurança zero trust avançada. Isso é importante porque

ajuda a garantir que todo acesso a dados sensíveis seja cuidadosamente controlado e monitorado, no contexto de risco apropriado, reduzindo o risco de acesso não autorizado, superexposição ou vazamento de dados.

Hoje, muitos provedores de serviços em nuvem (CSPs) e fornecedores de SaaS oferecem recursos nativos de DLP em suas plataformas. Essas soluções centradas na nuvem prontamente disponíveis são frequentemente escolhidas por organizações que buscam uma estratégia focada na nuvem ou aquelas que estão apenas começando sua jornada de proteção de dados. Embora essas soluções possam abordar os casos de uso específicos de proteção de dados em nuvem para os quais foram projetadas, elas podem não ter uma cobertura ampla e podem não ser tão abrangentes quanto as soluções legadas de DLP.



ATENÇÃO

Algumas empresas começam com essas soluções DLP nativas de nuvem porque podem ser rápidas e fáceis de implementar. No entanto, é importante abordar essas soluções com os olhos bem abertos, entendendo que elas podem não ser suficientes para atender a todas as suas necessidades de proteção de dados. Em alguns casos, as organizações podem se ver forçadas a adotar várias opções de DLP desconectadas e isoladas para casos de uso posteriores, levando a uma estratégia de proteção de dados fragmentada e potencialmente menos eficaz.

Tipo 2: nem todas as soluções de DLP integradas e entregues na nuvem são criadas igualmente

Quando se trata de escolher uma solução de DLP entregue em nuvem, lembre-se de que muitas soluções mais recentes no mercado apresentam deficiências significativas:

- » Elas podem oferecer ampla cobertura, mas carecem da profundidade tecnológica e dos recursos necessários para proteger os dados confidenciais de sua organização de maneira eficaz e precisa em todos os casos de uso modernos.
- » Elas podem oferecer algumas das metodologias e recursos mais recentes para alguns casos de uso e formatos de dados específicos, mas carecem da abrangência necessária para proteger os dados confidenciais de sua organização de forma completa.



ATENÇÃO

Algumas soluções de DLP entregues em nuvem mais recentes podem ser bem divulgadas, mas estão longe de serem tão sofisticadas e maduras quanto as soluções legadas de DLP que elas deveriam substituir.

É importante pesquisar e comparar minuciosamente as soluções de DLP para garantir que você escolha uma que atenda efetivamente às

necessidades da sua organização. Observe fatores como maturidade e sofisticação dos recursos de detecção de dados (por exemplo, quantos tipos de arquivos elas podem verificar e quantos identificadores de dados usam, incluindo tipos de dados localizados específicos para diferentes países), a variedade de canais que elas abrangem, sua capacidade de adaptação a riscos e ambientes em constante mudança e o nível de integração e personalização que oferecem.



DICA

Se você está pensando em usar uma solução de DLP entregue em nuvem para sua segurança de dados, pode estar se perguntando qual tipo é melhor para você. Eis o que você deve considerar:

- » **Amplitude de cobertura:** a DLP integrada como parte de uma solução de segurança de dados mais ampla normalmente incorpora DSPM, SWG, CASB ou NGFW e geralmente faz parte de um serviço de acesso de rede de confiança zero (ZTNA). Essas soluções são entregues na nuvem e integradas normalmente em um serviço de segurança de rede. Elas são limitadas em escopo e carecem, por exemplo, de proteção de dados para e-mails de saída, endpoints e um espectro maior de aplicações SaaS e suas instâncias específicas (contas corporativas versus contas pessoais).
- » **Limitações das soluções:** esteja ciente de que essas soluções podem não abranger todos os casos de uso modernos e tradicionais, como colaboração em nuvem com usuários externos, transferências de dados por e-mail pessoal ou rascunhos de e-mail, transferências de arquivos via USB, capturas de tela e fotos de documentos confidenciais, novos modelos de conformidade, dados em outros idiomas estrangeiros e formatos, entre outros. E ainda mais importante: elas podem ter capacidades de detecção mais fracas. Além disso, seus recursos de aprendizado de máquina (ML) e inteligência artificial (IA) podem ser decepcionantes.
- » **Precisão da detecção de dados confidenciais:** Muitas das soluções DLP mais recentes, entregues em nuvem, deixam a desejar em sua capacidade de detectar dados confidenciais com precisão e granularidade, estejam eles em infraestruturas on-premises (locais) ou na nuvem. Frequentemente, elas verificam apenas um número limitado de tipos de arquivo e não possuem a amplitude de identificadores de dados que as soluções mais maduras possuem. Essas soluções podem causar grande alvoroço ao focar em um ou dois recursos chamativos, mas no final das contas ficam aquém da sua capacidade de fornecer segurança de dados abrangente. O Netskope One Data Security fornece essa cobertura abrangente integrando DSPM e DLP em uma solução unificada.

Uma solução madura oferecerá milhares de identificadores de dados predefinidos, incluindo um amplo espectro de informações pessoalmente identificáveis (PII), passaportes, contas bancárias, informações bancárias internacionais, identidades nacionais, dados financeiros, dados médicos, biodados, informações específicas de cada setor, bem como idiomas localizados e identificadores personalizáveis. Ela também fornecerá uma ampla variedade de perfis de política predefinidos para dar suporte a casos de uso e requisitos de conformidade, como o RGPD (Regulamento Geral de Proteção de Dados) da União Europeia, a CCPA (California Consumer Privacy Act), o PCI DSS (Payment Card Industry Data Security Standard), o HIPAA (Health Insurance Portability and Accountability Act) e o GLBA (Gramm-Leach-Bliley Act), apenas para mencionar alguns.

- » **Integração a uma plataforma:** uma DLP entregue em nuvem deve se integrar totalmente a uma plataforma de segurança mais ampla para proteger dados confidenciais com eficácia em todo o contexto de risco disponível para usuários, dispositivos, redes, aplicações, comportamentos e destinos. Uma solução de DLP bem integrada usará inteligência de outros pontos de controle, como Análise de Comportamento de Usuários e Entidades (UEBA), SWG de última geração, CASB, ZTNA e DSPM, para entender de forma abrangente a postura de segurança de uma organização e os riscos associados a cada interação com dados confidenciais. Isso inclui estar ciente das instâncias específicas de aplicações e dispositivos SaaS em uso, distinguir entre identidades de usuários de contas de e-mail pessoais e corporativas, destinatários de compartilhamento de dados e muito mais. Esse nível de integração permite uma abordagem mais precisa e granular para detectar e proteger dados confidenciais.



DICA

Alguns fornecedores podem oferecer DLP como um complemento para seus principais produtos, mas sem a abrangência e a profundidade necessárias, essas soluções podem não fornecer o nível de proteção exigido pelas organizações.

Avalie e teste cuidadosamente os recursos de diferentes soluções de DLP e escolha uma que atenda às necessidades da sua organização, tanto agora quanto na amplitude de cobertura para o futuro. Conjuntos de recursos maduros e um fornecedor dedicado são essenciais para o sucesso. Confiar apenas no básico pode levar a imprecisões, detecção parcial e toneladas de falsos positivos.

Com mais de uma década de inovação contínua e dedicação total à segurança de dados, a Netskope é reconhecida como o padrão do setor em

comparação com outros fornecedores de SASE e de Borda de Serviço de Segurança (SSE). As seções a seguir analisam os recursos e funcionalidades que diferenciam o Netskope One Data Security.

Como o Netskope One Data Security mantém você seguro

O Netskope One Data Security é uma *solução integrada* abrangente entregue em nuvem que ajuda a proteger seus dados em todos os canais fundamentais, incluindo nuvens, redes, e-mails, endpoints e usuários em qualquer local. Ele foi projetado para ser baseado em risco e contexto, para que você possa confiar que seus dados estarão sempre seguros onde quer que se movam.

O Netskope One Data Security é totalmente integrado ao abrangente Netskope SSE descrito no capítulo 3 e entregue como parte de uma plataforma SASE completa. Isso significa que você obtém uma plataforma de segurança convergente nativa de nuvem que ajuda a eliminar pontos cegos, fornece consistência, melhora o desempenho e reduz custos e complexidade.

O Netskope One Data Security abrange todos os canais e transferência de dados, conforme mostrado na Figura 4-1, para que você tenha certeza de que suas informações confidenciais estarão sempre protegidas. Ele abrange:

- » Mais de 83.000 aplicações SaaS, com novas aplicações classificadas dinamicamente e todas as instâncias dessas aplicações
- » Todos os principais provedores de IaaS, incluindo Amazon Web Services (AWS), Google Cloud Platform e Microsoft Azure
- » Aplicações privadas no data center ou hospedadas na nuvem pública
- » Suas redes corporativas e filiais
- » Sua força de trabalho móvel
- » Todos os serviços de e-mail, on-premises e na nuvem, incluindo webmail
- » Todos os endpoints de seus funcionários, on- e off-premises

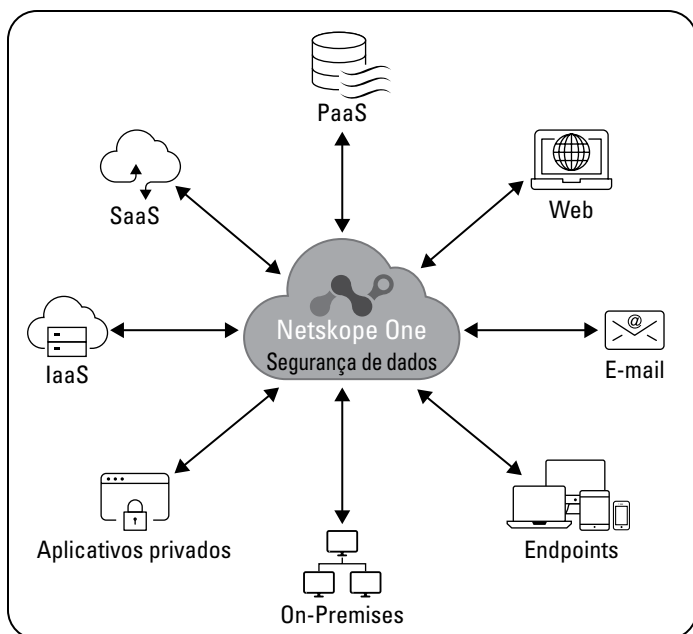


FIGURA 4-1: o Netskope One Data Security, que inclui DSPM e DLP unificados, garante que seus dados estejam seguros onde quer que estejam ou se movam.

Principais Diferenciais

Um mito sobre as soluções legadas de DLP é que elas são imprecisas; na realidade, os falsos positivos são um problema maior, que requer maior precisão para resolver. O capítulo 2 explica isso; ele também apresenta e explica ingredientes essenciais que podem ajudar os sistemas de DLP a atingir a precisão. Esta seção explica como a Netskope transformou esses ingredientes-chave em diferenciadores-chave e desenvolveu uma solução de segurança de dados unificada que pode ser personalizada e automatizada para atender às suas necessidades de negócios.

Cobertura completa de todos os canais importantes com políticas unificadas

Os dados confidenciais que se deslocam para todos os lugares fora das instalações corporativas tradicionais tornam-se mais difíceis de rastrear e proteger e são mais propensos à exposição intencional e não intencional. O Netskope One Data Security descobre, monitora e protege de forma abrangente dados confidenciais em movimento, em repouso e em uso em todo o ecossistema empresarial, incluindo aplicações SaaS, nuvens públicas IaaS, redes corporativas e filiais, força de trabalho móvel, serviços de e-mail e endpoints de funcionários.

Ele fornece políticas unificadas de segurança de dados para todos os locais onde os dados são armazenados, usados ou transferidos e entregues a partir de um serviço de nuvem centralizado.

Um único console, com controle de acesso baseado em função (RBAC), permite que o pessoal de segurança autorizado gerencie configurações de políticas, monitoramento, relatórios e resposta a incidentes para todos os canais por meio de um único painel de controle.

Detecção e proteção superiores de dados confidenciais

Os identificadores de dados são fundamentais para ajudar uma solução de DLP a identificar dados confidenciais com base em determinadas características, como palavras-chave descritivas, expressões regulares, número de dígitos, caracteres especiais, padrões, análise de proximidade e assim por diante. Ao comprar uma solução de DLP, certifique-se de que ela tenha recursos de identificação para cobrir todos os seus casos de uso atuais e futuros. Uma boa solução de DLP deve ser capaz de fornecer milhares de identificadores predefinidos para pesquisar e identificar com precisão a variedade mais ampla e até as menores variações de dados confidenciais. O Netskope One fornece todos esses recursos com ML e a capacidade de personalizar identificadores e modelos de políticas de forma granular, e garante que atenda a todas as suas necessidades de proteção de dados.



DICA

Não se concentre apenas nos identificadores de dados de que você precisa agora. Você precisa de uma solução pronta para o futuro que possa abordar tipos de dados, aplicações e regulamentações ainda a serem inventadas. Procure uma solução com milhares de identificadores de dados predefinidos e modelos de políticas para regulamentações de conformidade como GDPR e CCPA. E não se esqueça da capacidade de criar e editar identificadores de dados personalizados para atender às suas necessidades específicas.

Milhares de tipos de arquivo podem conter informações confidenciais, como arquivos compactados (ZIP, RAR, ISO etc.), apresentações, e-mails, imagens (BMP, JPG, PNG etc.), planilhas, design auxiliado por computador (CAD), postagens em redes sociais, formulários online, mensagens de bate-papo, vários anexos e gráficos. São muitos tipos diferentes de dados para acompanhar, então você quer uma solução de DLP que possa lidar com todos eles.

A escala de correspondência exata de dados (EDM) é um aspecto fundamental a ser considerado, especialmente se você tiver uma grande empresa — ou planeja um dia. A solução de DLP deve ser capaz de processar milhões ou até bilhões de registros com facilidade. Soluções de DLP modernas baseadas em nuvem, como o Netskope One, podem utilizar

computação em nuvem para executar análises de impressão digital de dados em larga escala, mesmo em endpoints, sem atrasar outros processos essenciais. Desta forma, todo o acervo de dados pessoais de colaboradores, clientes, parceiros, e muito mais, estará totalmente protegido.

Para garantir que seus dados confidenciais estejam ainda mais protegidos, procure recursos avançados de detecção — reconhecimento óptico de caracteres (OCR), IA, ML, impressão digital de arquivos e estratégias zero trust — em sua solução de DLP. Tudo isso está incluído no Netskope One Data Security (consulte o capítulo 2).

O Netskope One Data Security pode identificar com precisão dados confidenciais, mesmo que sejam armazenados em formatos modernos não estruturados, como imagens (capturas de tela e fotos) ou idiomas diferentes. Graças aos seus sofisticados classificadores de ML, a solução é capaz de discernir imagens confidenciais, como carteiras de motorista, cartões de crédito, identidades, contratos, patentes, documentos de fusões e aquisições (M&A) e cheques — mesmo que essas imagens estejam pouco nítidas, borradas, distorcidas e danificadas. Isso também reduz a carga de trabalho de suas equipes de segurança, identificando e protegendo automaticamente dados confidenciais.

O Netskope One Data Security possui uma variedade de ferramentas avançadas de classificação baseadas em ML, incluindo milhares de identificadores de dados. Ele verifica mais de 2.100 tipos de arquivos diferentes com políticas de detecção contextual, correspondência exata de dados altamente escalável, impressão digital de documentos estruturados e não estruturados, classificação precisa de imagens baseada em ML, OCR avançado e classificadores de dados baseados em IA/ML para descoberta e identificação de dados.

QUERIDA, VAMOS ENCOLHER A SUPERFÍCIE DE ATAQUE

As organizações que desejam proteger seus dados confidenciais contra ameaças cibernéticas devem eliminar qualquer lacuna na proteção. A *superfície de ataque* é o número total de vulnerabilidades potenciais ou pontos de entrada que os invasores podem aproveitar e que usuários internos podem usar intencionalmente ou maliciosamente. Limitar a superfície de ataque pode tornar mais difícil encontrar e explorar pontos fracos; fechar qualquer lacuna existente na proteção também pode reduzir significativamente o risco de uma organização sofrer um ataque bem-sucedido e uma exposição acidental. Garantir que todos os dispositivos, aplicações e redes estejam devidamente protegidos é essencial para eliminar quaisquer brechas que possam facilitar uma exposição arriscada.

Segurança de dados baseada em contexto e risco

A segurança eficaz de dados é totalmente voltada para o contexto. Ao monitorar o tráfego entre usuários e aplicações, você pode exercer controle granular e permitir ou impedir o uso de dados confidenciais com base em muitos fatores, como quem é o usuário, o que está tentando fazer e por que está fazendo. Essa abordagem centrada em dados é a melhor maneira de gerenciar riscos em empresas híbridas modernas.

A fadiga de resposta a incidentes e a interrupção dos negócios são problemas do passado com o Netskope One Data Security. Na verdade, ele vai além da abordagem estática de descobrir informações confidenciais e responder a políticas de violação predefinidas e fatores no contexto organizacional e riscos de segurança para viabilizar dinamicamente a proteção adequada com base em condições de mudança.

O Netskope One Data Security é integrado nativamente à abrangente solução Netskope Security Service Edge (SSE), uma plataforma de segurança nativa de nuvem totalmente convergente que consolida tecnologias de segurança, como SWG, CASB e UEBA, em uma plataforma nativa de nuvem integrada e unificada. Essa abordagem elimina pontos cegos na segurança, fornece consistência de política e reduz drasticamente os custos e a complexidade. A plataforma está continuamente ciente dos comportamentos dos usuários, geolocalizações, posturas de segurança, riscos de dispositivos, riscos e reputações de aplicações, instâncias de aplicações pessoais etc., e permite que a DLP adapte a resposta a incidentes para incidentes de segurança de dados reais, minimizando falsos positivos, a necessidade de triagem de incidentes e a interrupção dos negócios.

Você pode aumentar a visibilidade e a mitigação de riscos em todos os principais vetores com uma única solução convergente de proteção de dados SASE baseada em princípios zero trust e controles avançados de proteção de dados. Além disso, você pode simplificar a classificação de dados, a definição de políticas e o gerenciamento de incidentes com uma plataforma convergente que usa ML, comunicação completa e análises avançadas. E com políticas flexíveis e orientadas por contexto e um agente leve, você pode melhorar a agilidade para o usuário final e reduzir obstáculos.



LEMBRE-SE

Para garantir que seu programa de proteção de dados seja um sucesso, você deve treinar seus funcionários e incentivar práticas seguras de manuseio de dados. O Netskope One DLP oferece orientação em tempo real ao usuário e programas de conscientização para fazer exatamente isso. Ele também se integra aos principais sistemas de gerenciamento de aprendizado e possui um portal personalizável para o usuário final ser instruído sobre a proteção de dados através de autoatendimento.

Trabalhe de forma mais inteligente com DLP como parte de uma estratégia mais ampla de segurança de dados

O Netskope One DLP é entregue em nuvem, portanto, não depende de componentes on-premises (locais). Ele também oferece proteção sempre ativa e atualizada, eliminando a necessidade de atualizações manuais de software, comuns nas soluções legadas de DLP.

Com políticas de segurança de dados unificada, console único e RBAC, é fácil gerenciar configurações de políticas, monitoramento, comunicação e resposta a incidentes.

No passado, as empresas tinham que criar políticas separadas para canais separados (por exemplo, web, e-mail e cada aplicação individual), o que consumia muitos recursos e muito tempo. O Netskope One Data Security é um serviço de nuvem unificado e centralizado onde você pode definir uma única política para sua empresa e sincronizá-la automaticamente em todos os canais. Dessa forma, você pode criar sua política uma vez e não precisa replicá-la e refiná-la constantemente em diferentes lugares.



LEMBRE-SE

As soluções legadas de DLP precisavam de muitos administradores de sistema para criar e gerenciar políticas. A atual escassez de talentos torna importante escolher uma solução mais fácil de gerenciar.

Uma interface de usuário (IU) centralizada e um console de gerenciamento unificado também são cruciais para uma resposta eficaz e eficiente a incidentes. Você pode ter tido consoles separados para ferramentas on-premises (locais) e entregues em nuvem, o que pode ser confuso e demandar muito tempo para gerenciar. Ainda hoje, alguns fornecedores de DLP mais recentes ainda usam uma abordagem de vários consoles, o que pode complicar o monitoramento do gerenciamento. Com o Netskope One Data Security, você recebe notificações de todas as violações em um só lugar, a detecção de dados confidenciais e a resposta a incidentes são entregues de forma consistente e em tempo real, para que você possa responder de forma rápida e eficaz a possíveis ameaças.



DICA

Uma IU centralizada e um console de gerenciamento unificado facilitam o acompanhamento de tudo e agilizam o processo de resposta a incidentes.

- » Priorizando as ameaças à segurança de dados que tiram seu sono
- » Identificando e abordando vulnerabilidades dentro e fora da sua empresa
- » Escolhendo um provedor e uma solução em que você pode confiar

Capítulo 5

Dez (ou mais) fatores para uma transição bem-sucedida para a segurança de dados unificada

Substituir implementações de segurança consolidadas há tempo, como a Prevenção de Perda de Dados (DLP) legada, pode parecer intimidador. Sua iteração atual pode ser o resultado de anos de processos complicados e interligados. Como um castelo de cartas, cada elemento toca o outro, e a remoção de um elemento ameaça derrubar toda a estrutura.

Não se deixe intimidar! Vale a pena buscar uma transformação digital inovadora. E a mudança não precisa acontecer da noite para o dia. Dê pequenos passos, use seus investimentos atuais com sabedoria e você estará no caminho certo para uma solução abrangente que protege dados confidenciais em todas as plataformas, seja on-premises ou na nuvem.

Neste capítulo, oferecemos dez (ou mais) passos a serem seguidos na transição para a segurança de dados unificada.

Avalie suas necessidades de segurança de dados

Reserve um tempo para avaliar completamente o ambiente de tecnologia atual da sua organização. Identifique e compreenda quais dados devem ser protegidos, quais serviços e repositórios você está usando para armazenar e processar informações confidenciais e como os departamentos e indivíduos estão usando esses serviços. Faça com que sua equipe de segurança identifique e avalie especificamente todas as aplicações corporativas, serviços de e-mail, ferramentas de colaboração, locais de rede, práticas de trabalho híbrido dos usuários, dispositivos de conexão e processos de negócios para mapear fluxos de dados e determinar como os dados são compartilhados entre funcionários ou terceiros.



DICA

Não se limite à equipe de segurança. O diretor de dados (CDO), a equipe jurídica e o pessoal de recursos humanos (RH) da sua empresa estão entre as outras partes interessadas que podem fornecer insights sobre como sua empresa usa os dados.

Examine todas as categorias de dados armazenados e todas as transações envolvendo dados que se movem pelas redes. Descubra quanta prioridade você precisa dar à proteção de vários tipos de dados em sua organização. Esta etapa pode representar uma vitória rápida para organizações que precisam de suporte para conformidade regulatória ou que necessitam de novas implantações de DLP devido a sistemas legados ineficazes.

Identifique e mitigue seus maiores riscos

Ao procurar fazer a transição para uma solução de proteção de dados entregue em nuvem, determine quais áreas de seu ambiente de tecnologia atual apresentam os maiores riscos. Pense no compartilhamento não intencional de dados, exfiltração maliciosa e outras ameaças cibernéticas baseadas em nuvem associadas a aplicações corporativas SaaS (software como serviço), e-mail em nuvem e IaaS (infraestrutura como serviço).



DICA

A solução de CASB (corretor de segurança de acesso à nuvem) líder de mercado da Netskope incorpora a DLP como seu componente principal para proteger os dados em aplicações de nuvem autorizadas pela empresa e (você está se enganando se pensa que não tem) aplicações não autorizadas.

Escolha seu fornecedor de segurança de dados com sabedoria

Você deve escolher um fornecedor que atenda às necessidades da sua empresa em todos os ambientes hoje e no futuro previsível.



DICA

A Netskope é o único fornecedor que oferece cobertura abrangente para todas as necessidades de segurança de dados e além. Isso inclui proteção de dados em repouso, em trânsito e em uso em nuvens e on-premises (locais), DLP de endpoint, DLP de e-mail, DLP de rede para web e para e-mail, DLP para SaaS e IaaS e DLP para aplicações privadas. Essa cobertura abrangente de todos os fluxos de dados modernos garante que as organizações tenham visibilidade máxima em todo o seu sistema, bem como em locais não confiáveis.

Avalie cuidadosamente a profundidade dos recursos de cada solução — por exemplo, quantos e quais tipos de arquivo a solução pode verificar, a capacidade de entender formatos de imagem e a cobertura da mais ampla variedade de dados confidenciais, incluindo identificadores específicos internacionais e de países. Considere a capacidade do sistema de utilizar o máximo possível de riscos e contexto empresarial e, portanto, de tomar decisões de resposta a incidentes automatizadas e bem informadas com cada uso de dados confidenciais de forma adaptativa.

Basicamente, certifique-se de não adotar uma abordagem superficial à segurança de dados, que criará mais problemas do que soluções.

Proteja seus serviços de e-mail e aplicações de colaboração

Descubra o poder do e-mail baseado em nuvem e proteção SaaS com o Netskope One Data Security. Essa solução abrangente foi projetada para proteger todas as informações confidenciais da sua empresa, incluindo e-mails confidenciais enviados e comunicações assíncronas por meio de aplicações de colaboração baseadas em SaaS, como o Slack e o Microsoft Teams. Com interfaces de programação de aplicativos (APIs), proteção em tempo real integrada, proteção para colaborações externas e até mesmo consciência contextual — como distinguir entre e-mails pessoais e instâncias de SaaS versus instâncias corporativas dos mesmos serviços —, você pode ter certeza de que seus dados corporativos estarão seguros em qualquer situação. Com a ajuda da Netskope, você ficará tranquilo quando se trata de colaboração e comunicação.

Proteja seu e-mail baseado em nuvem

Descubra o poder da proteção de e-mail baseado em nuvem com o Netskope One DLP. Esta solução abrangente de DLP foi projetada para proteger todas as informações confidenciais de sua empresa, protegendo contra ataques mal-intencionados e compartilhamento não intencional de dados. Com APIs, proteção em tempo real em linha e até mesmo proteção de dados por meio de instâncias de e-mail pessoal, você pode ter certeza de que seus dados corporativos estarão seguros, não importa o que aconteça. Com a ajuda da Netskope, você terá tranquilidade na hora de migrar seu serviço de e-mail para a nuvem.

Dados seguros em movimento

Os dados transferidos entre diferentes locais, conexões, serviços e dispositivos, como redes domésticas, escritórios corporativos, filiais, dispositivos corporativos e dispositivos pessoais, podem ser difíceis de gerenciar e proteger. As soluções tradicionais de DLP conectadas por proxy nem sempre oferecem proteção suficiente quando se trata de dados em movimento.



DICA

A Netskope fornece segurança de dados unificada por meio da plataforma Netskope One, que protege a transmissão de dados confidenciais entre locais on-premises e/ou na nuvem. Dessa forma, você terá a segurança máxima para suas transações de dados, incluindo todos os benefícios dos princípios zero trust, amplo contexto de risco e nenhum dos aborrecimentos de configurações obscuras de hardware. Com o Netskope One Data Security, você pode garantir que seus dados estejam seguros o tempo todo, em qualquer lugar.

Proteja os dados nos dispositivos de endpoint dos funcionários

Embora cada vez mais dados sejam armazenados na nuvem, ainda é importante garantir que arquivos confidenciais não sejam perdidos ou roubados em endpoints que podem ou não estar conectados a uma rede corporativa ou podem não estar conectados de modo algum.



DICA

Quer os dados confidenciais sejam criados no endpoint ou baixados da nuvem, o Netskope One DLP pode ajudar com isso. Essa solução de endpoint leve oferece todos os recursos avançados de DLP, como classificadores baseados em aprendizado de máquina (ML), reconhecimento

óptico de caracteres (OCR), impressão digital de arquivos, correspondência exata de dados (EDM) e muito mais, com utilização mínima de recursos, porque utiliza a nuvem. Ela permite uma variedade de casos de uso, incluindo detecção de dados transferidos via USB e fornece proteção de dispositivo USB e outras políticas de controle de dispositivo para garantir que seus dados confidenciais permaneçam seguros, independentemente de onde seu pessoal esteja conectado.

Atenha-se ao que funciona ao planejar o futuro

Se você investiu recentemente em recursos de DLP de um provedor de serviços em nuvem ou fornecedor de SaaS, mantê-los por um curto período pode ser uma boa ideia. Por exemplo, se um fornecedor de SaaS já está fazendo um bom trabalho protegendo suas aplicações administrativas, você não precisa mudar imediatamente.



ATENÇÃO

Mas fique atento ao ponto em que você está gerenciando muitas políticas distintas e desconectadas. Se você deseja expandir a proteção de dados em várias nuvens e aplicativos SaaS, pode acabar lidando com muitos consoles e políticas diferentes.



DICA

O Netskope One DLP oferece uma solução mais simples: um console com políticas consistentes que podem proteger seus dados, não importa onde sejam armazenados ou acessados.

Desbloqueie a segurança de dados abrangente

O Netskope One oferece uma abordagem moderna para segurança de dados que é mais eficiente e eficaz do que nunca. Tecnologias avançadas de detecção, como ML, impressão digital de dados e reconhecimento de imagem, são usadas em todo o potencial e em escala sem precedentes, mesmo nos endpoints, pois a capacidade de computação é fornecida pela nuvem. O console único com políticas unificadas simplifica o gerenciamento de todas as necessidades de proteção de dados da organização. A coleta e análise de inteligência de risco e informações contextuais sobre usuários, dispositivos, dados, redes, nuvens e comportamentos permitem exclusivamente que o Netskope One DLP avalie cada interação com dados confidenciais e adapte dinamicamente a resposta a cada violação de política específica. Essa nova abordagem oferece suporte à

colaboração segura e práticas modernas de compartilhamento de dados, minimiza falsos positivos e produz resultados de proteção de dados mais precisos, tudo isso sem prejudicar a produtividade.



LEMBRE-SE

O Netskope One Data Security é nativamente integrado à plataforma geral do Netskope One SSE, por isso está sempre ciente dos riscos comerciais, comportamentos e vulnerabilidades de segurança. Com o Netskope One, as organizações estão sempre cientes dos riscos comerciais, comportamentos e vulnerabilidades de segurança.

Preserve o conhecimento institucional

A transição para uma nova DLP baseada em nuvem pode parecer assustadora, mas não precisa ser. Aproveite a experiência e o conhecimento das pessoas que mantiveram seu sistema legado de DLP, incluindo seus administradores de políticas e equipe de resposta a incidentes. A experiência deles pode ajudar a garantir que as melhores práticas sejam replicadas durante a transição para um sistema baseado em nuvem. Essa experiência também pode ajudar sua organização a atender às expectativas tecnológicas, produzindo perfis de política de conformidade e desenvolvendo novos fluxos de trabalho de correção de incidentes.



DICA

O Netskope One DLP ajuda a reduzir as demandas de sua equipe de DLP, para que suas equipes de segurança gastem menos tempo gerenciando incidentes frustrantes e mais tempo se concentrando em iniciativas proativas que mantêm sua empresa segura.

Valorize mais a maturidade do que a propaganda

O sucesso exige mais do que conhecimento técnico. Desde o desenvolvimento de métricas para gerenciamento de alto nível até orientações e itens de ação para a equipe, você tem muito a considerar. Você deve contar com as equipes de suporte de seu fornecedor para ajudar a estruturar sua jornada e, finalmente, ajudá-lo a destravar o valor da inovação da empresa e fazer a jornada valer a pena!



Segurança ~~ou~~ e desempenho de rede modernas.

Sem abrir mão de nada.

Nós protegemos os dados, simplificamos
a complexidade e melhoramos
ativamente a experiência do usuário.



Saiba como



Proteja seus dados onde quer que eles estejam e se movam, minimizando os obstáculos para os negócios

A rápida adoção da nuvem e a tendência de trabalhar de qualquer lugar tornam as técnicas de proteção de dados, outrora de ponta, lamentavelmente inadequadas. Os esforços de segurança de dados devem proteger os dados de forma consistente a todo momento, onde quer que estejam. A solução ideal para a segurança de dados moderna deve ser construída para a nuvem — não adaptada para casos de uso em nuvem. Ela deve aplicar técnicas zero trust, reduzir a complexidade e fornecer imposição consistente de políticas — em todos os lugares — e sem causar obstáculos excessivos para os negócios ou sobrecarregar a equipe de segurança com falsos positivos.

Tópicos deste livro...

- Avalie a segurança de dados existente
- Implemente uma abordagem unificada focada em nuvem
- Gerencie operações de segurança por meio de um único painel de controle
- Impeça exfiltrações de dados não autorizadas antes que elas aconteçam
- Minimize os falsos positivos para reduzir obstáculos para os negócios
- Aplique os princípios zero trust para máxima proteção



Cover image: © matejmo/Getty Images

Acesse [Dummies.com](https://dummies.com)®

para ver vídeos, fotos passo a passo, artigos de instruções ou para fazer compras!

ISBN: 978-1-394-42070-4

Proibida a revenda

para
leigos[®]
A Wiley Brand



WILEY END USER LICENSE AGREEMENT

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