eBook

5 requisitos para um DLP moderno

netskope

No mundo preparado para a nuvem de hoje, impulsionado pela transformação digital e pelo trabalho híbrido, as organizações devem alinhar as iniciativas de segurança de dados às tendências modernas que mudam na velocidade da nuvem. Além disso, cada organização tem necessidades específicas de proteção de dados e casos de uso específicos, porque os programas de proteção de dados nunca são exatamente os mesmos. É por isso que apenas uma arquitetura de prevenção contra perda de dados (DLP) fornecida na nuvem pode garantir alta flexibilidade, grande escalabilidade e poder de computação ilimitado. A nuvem significa também estar sempre atualizado, com proteções sempre ativas e atualizações disponíveis em tempo real. Uma tecnologia DLP na nuvem como serviço é claramente a abordagem certa para a proteção de dados corporativos, mas não deve ser o único critério a ser considerado na migração para uma estratégia efetiva de proteção de dados.

Uma tecnologia DLP precisa ser adaptativa, repleta de recursos, ampla em cobertura e profunda em eficácia. Ela também precisa fornecer um alto grau de eficácia para garantir proteção de dados precisa para qualquer tipo de dados, em todos os ambientes e contra todos os riscos de perda de dados.

Existem diretrizes de arquitetura e recomendações de tecnologia úteis que sempre devem ser consideradas antes de passar de uma implantação DLP existente para uma que atenda aos requisitos modernos de trabalho híbrido:

01

Extensão da cobertura

Você não pode proteger o que não pode ver, e os dados hoje estão fluindo por muito mais ambientes do que antes. O Legacy Enterprise DLP, tradicionalmente implantado na rede física, oferece ampla cobertura dos canais de dados on-premises, incluindo transmissões da Web, SMTP de e-mails e endpoint. É razoável esperar que uma solução moderna na nuvem estenda a proteção a repositórios na nuvem, como aplicações SaaS, IaaS e e-mail na nuvem, além de garantir cobertura em ambientes on-premises, como redes, endpoints e e-mails. É sempre recomendável certificar-se que uma solução DLP na nuvem forneça uma cobertura corporativa completa para a nuvem e os canais on-premises tradicionais. Nesse sentido, também é importante saber que a maioria das soluções DLP na nuvem foi desenvolvida para a nuvem para resolver apenas os casos de uso na nuvem e não abrange determinados canais on-premises, como endpoints.

01

Atualmente, existem muitos casos de uso que são fundamentais e devem ser abordados adequadamente, como a transferência de dados confidenciais entre milhares de aplicações SaaS de risco não sancionadas ou para instâncias pessoais de aplicações SaaS sancionadas, como uma conta pessoal de Gmail ou uma instância pessoal do OneDrive, ou para aplicações privadas na nuvem pública ou no data center. Para a empresa moderna altamente distribuída, composta por várias filiais e uma força de trabalho remota híbrida, o DLP deve proteger todas as transmissões de dados de qualquer local e dispositivo, incluindo dispositivos gerenciados e não gerenciados e até a IoT. A transferência de dados confidenciais através de endpoints para um USB também é um veículo de perda significativa que deve ser controlado, mesmo quando esses endpoints não estão on-line. E-mails enviados, de natureza confidencial, são um outro grande vetor de perda de dados, bem como comunicações confidenciais em aplicações de colaboração como Slack e Teams.

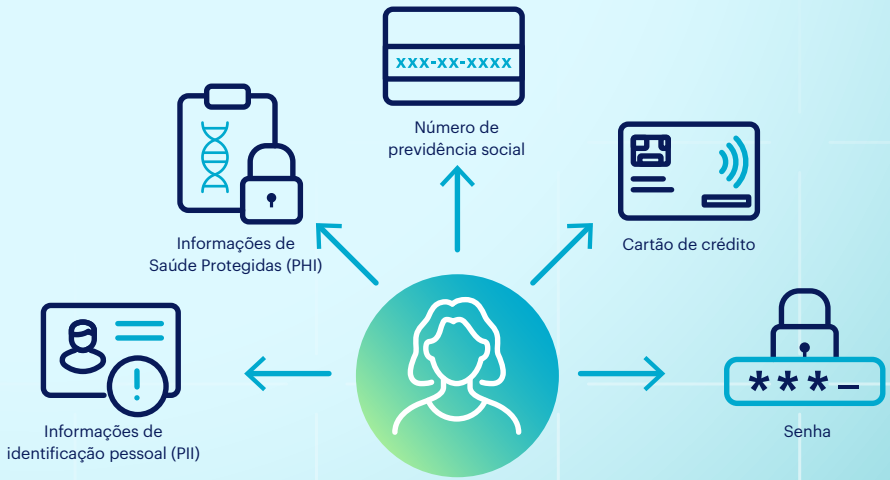
02

Principais recursos de detecção de dados

A visibilidade precisa dos dados é uma necessidade tática para avaliar todo o ambiente operacional e implementar a estratégia de proteção ideal. Tudo começa com a descoberta e a classificação de todos os dados confidenciais, incluindo informações de identificação pessoal (PII) estruturadas e não estruturadas, propriedade intelectual (PI), informações confidenciais e segredos comerciais.

Como a classificação manual de dados pelo proprietário dos dados pode ser um processo não confiável, essa tarefa também precisa ser automatizada em DLP por meio de um conjunto completo, e não parcial, de mecanismos de detecção. Esses mecanismos definem as políticas de detecção ou os perfis de dados predefinidos da organização. Em detalhe:

- Os **Identificadores de dados** foram e ainda são essenciais para qualquer solução DLP. Eles devem ser capazes de identificar milhares de tipos diferentes de dados confidenciais com base em critérios de correspondência descritos que geralmente caracterizam objetos como SSN, dados de cartão de crédito ou números de passaporte, como número de dígitos, padrões de texto, sequências, separações e palavras-chave de proximidade. É fundamental ter recursos de expressão regular (regex), mas não pode ser algo simples como, por exemplo, assinalar um quadrado. Mais tipos de dados e casos de uso modernos surgiram com novos requisitos de conformidade que exigem proteger a privacidade dos indivíduos de maneira mais ampla. Na realidade, um grande número de identificadores de dados predefinidos é o primeiro elemento a ser considerado, mas também deve-se levar em consideração a granularidade das personalizações das regras, como níveis de severidade, extensão das verificações de proximidade, lógica booleana, etc..



02

- O número de **tipos de arquivo** suportados é outro elemento importante. Existem milhares de tipos de dados que podem conter informações confidenciais: Textos, Apresentações, Emails, Imagens e Capturas de Tela, Planilhas, CAD, Postagens Sociais, Formulários On-line, Mensagens via Slack e de outros canais de chat, Encapsulamento, Anexos, Gráficos e Imagens como JPEG e PDF, etc.
- Os **Classificadores de dados de Inteligência Artificial/Aprendizado de Máquina (AI/ML)** ajudam na descoberta e na identificação de dados. As regras definidas manualmente são a base da detecção de dados, mas no mundo moderno, os mecanismos automatizados fornecem uma assistência valiosa e tornam a detecção e a categorização de dados confidenciais mais precisas. Elas também se adaptam às condições de mudança e identificam semelhanças em conteúdo.
- A **correspondência exata de dados (EDM)** é um método tradicional, mas quase infalível, projetado para detectar informações específicas provenientes de fontes de dados estruturados, como planilhas e bancos de dados. Com a EDM, uma solução DLP pode identificar e indexar conjuntos de dados de registros confidenciais, informações que, quando reunidas, podem identificar um indivíduo, como nomes completos de clientes, números de CPF, endereços, números de identificação, etc., ou registros financeiros que definem ativos financeiros de uma pessoa, como números de cartão de crédito ou números de contas bancárias, até mesmo informações sobre saúde ou identificação de produtos e bancos de dados de preços. Essas informações indexadas devem ser rastreadas e encontradas em qualquer lugar onde se espera que os fluxos de dados aconteçam.

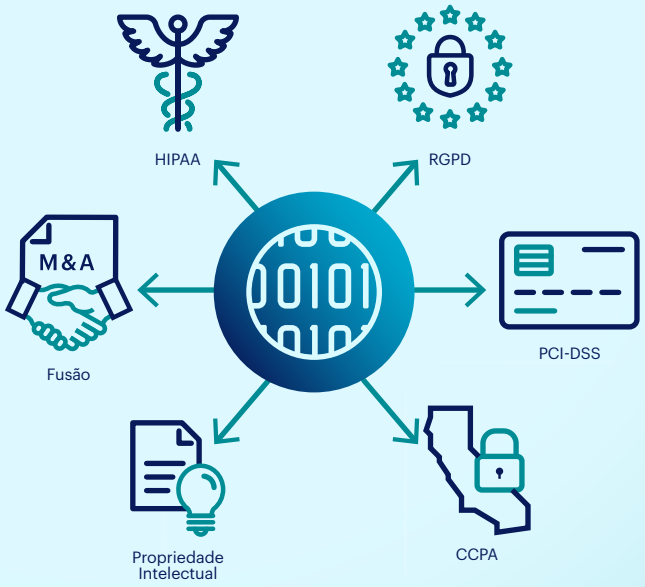
Uma nota sobre a EDM

Para que a EDM seja efetiva e precisa, ela deve ser capaz de usar condições granulares para reunir vários dados indexados e combinar com os campos de dados mais importantes de um registro específico. A alta escala da EDM é um fator muito importante, especialmente para grandes empresas e organizações que pretendem expandir no futuro. Milhões ou mesmo bilhões de registros devem ser aceitos.

03

Criação de perfil de dados futuros

Não procure apenas por identificadores de dados de que você precisa agora. Procure milhares de identificadores de dados predefinidos, incluindo padrões localizados, como cartões de identificação com base no país, pois suas necessidades futuras provavelmente se expandirão junto com o tamanho da sua organização e a maturidade da proteção de dados. Procure modelos de conformidade regulatória que você precisa suportar para verificar se os mais recentes estão todos lá — RGPD, CCPA, IDP, PCI, PHI, para citar apenas alguns dos tipos e dos regulamentos mais conhecidos. Entenda o nível de comprometimento do fornecedor para acompanhar os requisitos de conformidade mais recentes e determine se o fornecedor provavelmente expandirá esses requisitos no futuro. A capacidade de editar regexes ou identificadores existentes ou criar identificadores de dados personalizados com controles granulares é fundamental, porque cada organização tem necessidades diferentes, como um tipo específico de informação que é confidencial apenas para essa organização específica.



04

Recursos avançados de detecção de dados

Ao longo dos anos, os dados também evoluíram significativamente, crescendo em volume, variedade e velocidade, e estão mais desestruturados do que nunca. A introdução de novos tipos de dados e maneiras modernas de compartilhamento e de transmissão de dados, o enorme crescimento nos volumes de dados e novos requisitos de conformidade exigem formas avançadas de detecção de informações confidenciais. As soluções legadas de DLP introduziram recursos avançados de detecção no passado, mas começaram a não conseguir mais fornecer resultados de detecção precisos devido à falta de escalabilidade e capacidade de processamento. Como consequência, elas geram cada vez mais falsos positivos que atrapalham os fluxos de negócios e sobrecarregam as equipes de resposta a incidentes.

Por outro lado, a maioria das soluções recentes de DLP em nuvem ainda pode ser imatura e não comprovada em termos de eficácia. É importante verificar a presença e o nível de sofisticação dos seguintes recursos avançados de detecção:

- No mundo atual, os usuários acham muito conveniente tirar fotos de documentos, formulários, carteiras de identidade, quadros brancos e até mesmo fotos de outras fotos. Por exemplo, as capturas de tela são um veículo muito comum para capturar informações rapidamente e compartilhá-las imediatamente com um colega. Como consequência, o **Reconhecimento ótico de caracteres (OCR)** e o reconhecimento de imagem baseado em inteligência artificial estão se tornando cada vez mais essenciais em uma estratégia de proteção de dados moderna e voltada para o futuro. Com o OCR, uma solução DLP pode extrair informações textuais de uma imagem e aplicar a classificação de dados com base nas políticas de detecção existentes.
- A **classificação de imagens por IA e ML** é fundamental para reconhecer tipos comuns de arquivos e documentos, como cartões SSN, patentes e documentos de fusões e aquisições, formulários de impostos, código-fonte, capturas de tela em desktops, passaportes e outras identidades, etc., sem necessariamente extrair o conteúdo que esses documentos contêm. Esses métodos de detecção devem fornecer um alto nível de sofisticação para conseguirem reconhecer imagens por meio de variações como partes de conteúdo desfocadas, amassadas e danificadas, com informações que podem ser difíceis de ler com clareza. Isso ocorre porque as fotos e as capturas de tela podem ter sido tiradas rapidamente e com condições de luz fracas ou muito fortes ou porque um documento pode estar danificado e envelhecido.

04

- A **impressão digital de arquivos e documentos** é um outro recurso avançado que muitas organizações consideram vital. Determinados documentos de missão crítica, propriedade intelectual e arquivos altamente confidenciais devem ser protegidos a todo custo contra a transferência total ou parcial não autorizada de dados e cópias duplicadas. A impressão digital de arquivos pode indexar documentos inteiros e detectar cópias exatas ou mesmo parciais das informações que eles contêm com certos graus de semelhança, quando esse conteúdo é encontrado em ambientes e canais de transmissão considerados de risco, como um upload para uma instância privada de uma aplicação de e-mail.

05

Proteção de dados com reconhecimento de risco, um modelo pronto para zero trust

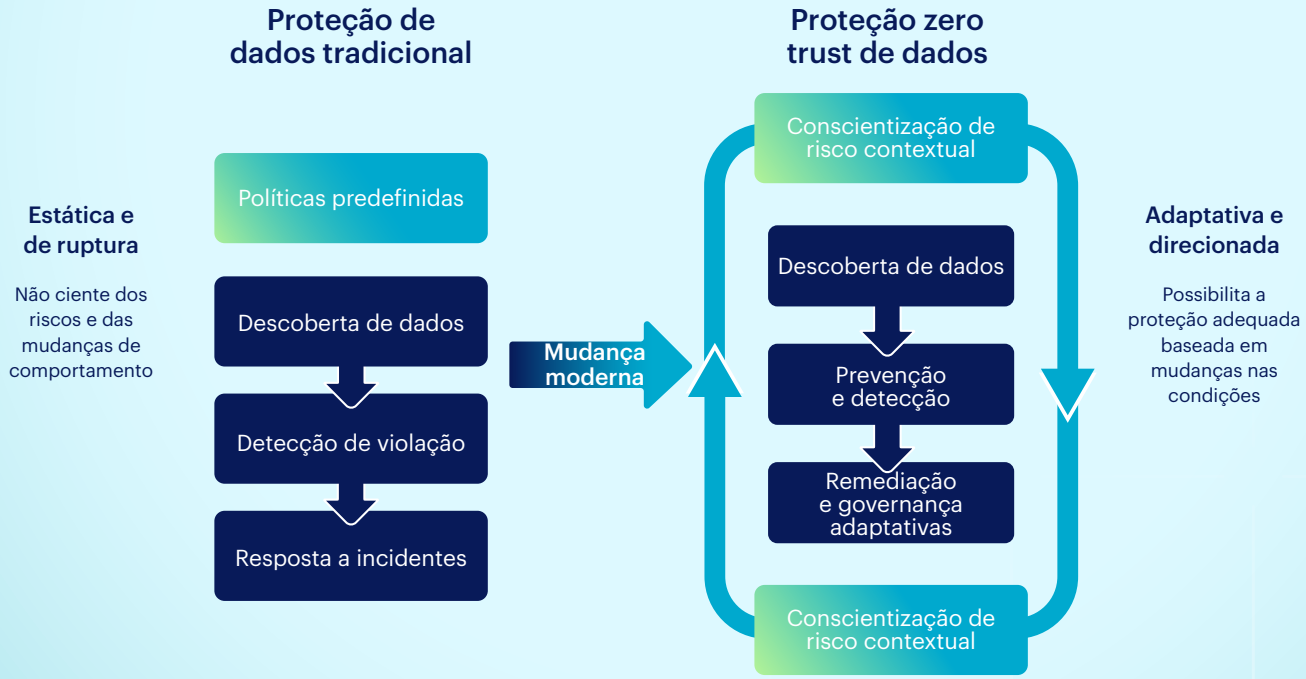
A transformação digital mudou nosso paradigma operacional para sempre e precisa de um modelo que a atenda. Zero trust é uma estratégia moderna com controles de segurança para os próprios dados como um novo perímetro e substitui a confiança implícita por avaliação de risco contínua e adaptativa para se adaptar constantemente às mudanças nas condições de risco. Os controles de dados causavam problemas operacionais e dificultavam a criação de valor porque não tinham contexto. É por isso que o DLP tradicional não conseguiu ser eficaz: Não havia contexto de negócios e reconhecimento de riscos suficientes para estabelecer a confiança necessária para evitar as movimentações de dados. A maioria das decisões de remediação de incidentes em DLP precisava ser tomada manualmente pela equipe de resposta a incidentes, a qual também carecia de contexto comportamental e de risco suficiente. Por causa disso, o DLP tradicional é hoje visto como um inibidor de negócios, especialmente quando o modo de bloqueio está ativado, e não uma solução eficaz de proteção de dados. Na verdade, a maioria das organizações está usando DLP como uma ferramenta de descoberta de dados e conformidade, trabalhando em modo de monitoramento para evitar problemas.

Com a aplicação de zero trust, esses desafios são resolvidos. A tecnologia de proteção de dados é necessária para mudar de um modelo estático composto de políticas fixas predefinidas, sem contexto ou reconhecimento de riscos e comportamentos em mudança, para uma abordagem zero trust dinâmica e adaptativa que pode usar o contexto de segurança e permitir continuamente a ação de proteção adequada, de forma automática com base em condições em constante mudança.

A resposta automatizada de proteção de dados exige processos definidos e políticas granulares, juntamente com regras claras de engajamento, quais medidas tomar sob quais condições com qual grau de confiança. O DLP deve se integrar com o maior número de pontos de controle de segurança, ingerir continuamente seus registros e descobertas e usá-los dinamicamente. Um DLP preparado para zero trust deve levar em consideração os riscos organizacionais dos usuários, dispositivos, dados, redes e aplicações para um bom reconhecimento dos riscos e sempre fornecer a ação de remediação correta. Por exemplo, o monitoramento comportamental dos usuários, dispositivos e aplicações proporciona informações valiosas sobre atividades anômalas dos usuários, ações potencialmente maliciosas, aplicações de risco, locais de conexão inseguros, posturas inseguras e indicadores de comprometimento.

05

Para ser realmente eficaz, uma solução zero trust de proteção de dados precisa monitorar o que está acontecendo e quem está fazendo o quê em toda a infraestrutura corporativa, incluindo nuvens, usuários remotos e dispositivos não gerenciados.



Mais informações

A Netskope, líder global em segurança cibernética, está redefinindo a segurança da nuvem, dos dados e da rede para ajudar as organizações a aplicar os princípios de Zero Trust para proteger os dados. A plataforma Netskope Intelligent Security Service Edge (SSE) é rápida, fácil de usar e protege pessoas, dispositivos e dados onde quer que eles estejam.

Saiba como a Netskope ajuda os clientes a estarem preparados para tudo na sua jornada de proteção de dados

netskope