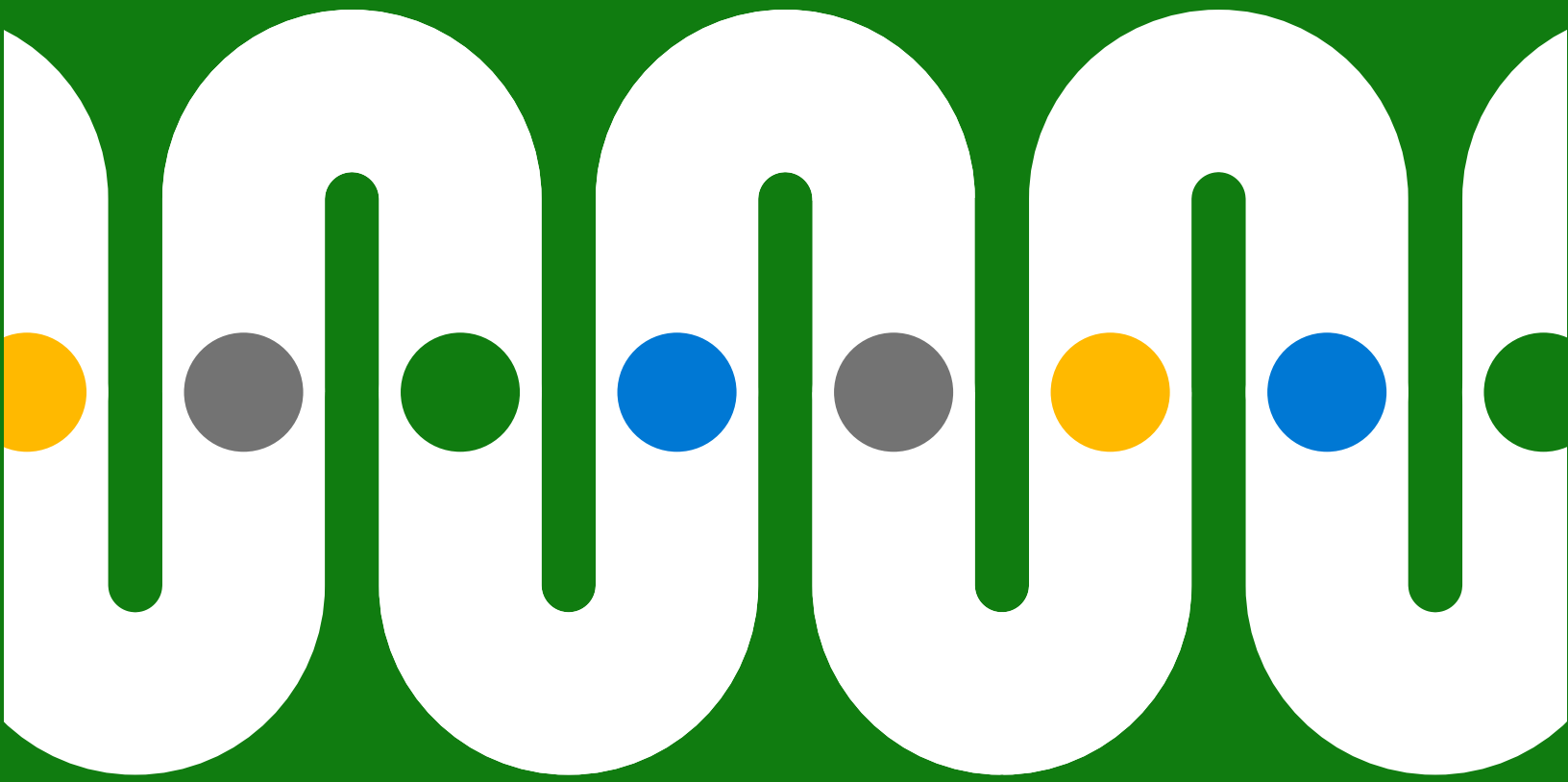
Microsoft Security

Três etapas para proteger seus dados de ponta a ponta



Sumário

Uma pesquisa com tomadores de decisão de conformidade mostrou que 95% estavam preocupados com os desafios de proteção de dados.[2]

Introdução

As organizações têm visto um enorme aumento em sua pegada digital com o trabalho híbrido, estendendo-se bem além do escritório tradicional.

Isso levou a mais fragmentação de dados e exfiltração, tudo complicado pelo rápido crescimento em uma infinidade de aplicações, dispositivos e locais de trabalho. Muitos trabalhadores também trocaram funções em busca de maior satisfação ou flexibilidade, e isso é adicionado a esses desafios, criando novos pontos cegos em propriedades de dados cada vez maiores.[1]

Todos esses fatores fazem os CIOs e CISOs repensar em sua abordagem de proteção de informações. Em uma pesquisa de rastreamento com mais de 500 tomadores de decisão de conformidade dos EUA, quase todos (95%) estavam preocupados com os desafios de proteção de dados.[2]

[1] "Como a Microsoft pode ajudar a reduzir o risco interno durante a grande reorganização, Alym Rayani", Segurança da Microsoft. 28 de fevereiro de 2022.

[2] "Pesquisa de setembro de 2021 com 512 tomadores de decisão de conformidade dos EUA patrocinada pela Microsoft e feita pela Vital Findings".

As equipes de TI e de segurança estão procurando maneiras melhores de gerenciar todo o ciclo de vida dos dados, em ambientes de nuvem híbrida, multinuvem e na infraestrutura local. Essa abordagem de ponta a ponta envolve três etapas principais:

Etapa 1: Identificar dados

Determine onde seus dados estão, que tipo de dados ele são e como eles estão sendo usados ou compartilhados

Etapa 2: Classificar dados

Classifique e rotule dados para que você saiba as políticas certas e a mitigação de riscos a serem aplicadas

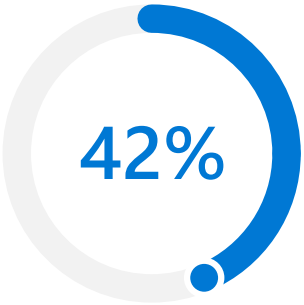
Etapa 3: Evitar a perda de dados

Estabeleça um equilíbrio entre a redução de riscos e a flexibilidade para seu pessoal com detecção e controle inteligentes

A meta dessa abordagem? Fechar lacunas e minimizar o risco sem sacrificar a produtividade.

Etapa 1

Identificar dados



Quando perguntadas o quanto de seus dados são incompreensíveis, 42% das organizações disseram pelo menos metade.[3]

Esses dados incompreensíveis podem assumir muitas formas, desde anexos de email e registros de chamadas do cliente até logs de computador e filmagens de vídeo.

Se você não puder identificar seus dados – onde eles estão, de que tipo eles são ou como eles estão sendo usados e compartilhados – será impossível aplicar as políticas ou a proteção corretas.

As organizações modernas geram continuamente grandes quantidades de dados. Não são apenas documentos, emails e mensagens, mas tudo, desde filmagens de segurança até dados de geolocalização, agravado pela proliferação entre aplicativos, dispositivos e armazenamento, na infraestrutura local e na nuvem.

A identificação de todos esses dados pode ser difícil, e 42% das organizações dizem que pelo menos metade de seus dados são incompreensíveis.[3] Ou seja, informações coletadas mas desconhecidas ou não utilizadas para fins comerciais. Às vezes, os dados ficam incompreensíveis quando o trabalhador que os criou alterna projetos ou funções; muitas vezes, simplesmente não há sistemas em vigor para identificar dados no ponto de criação ou modificação.

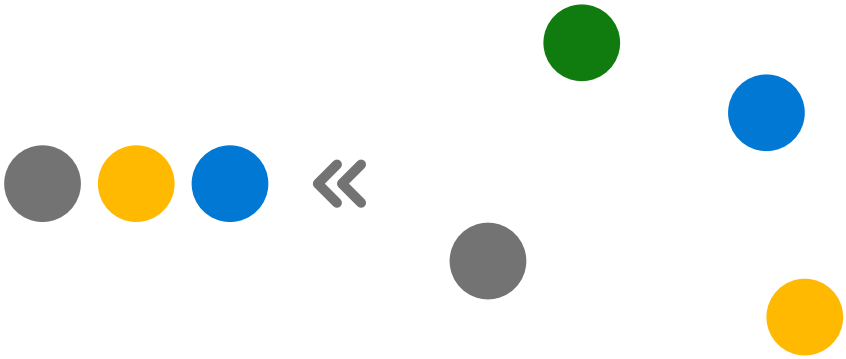
[3] "2022 State of Data Governance and Empowerment Report", Enterprise Strategy Group. Julho de 2022.

Deseja criar um fluxo de trabalho de descoberta de ponta a ponta em uma única plataforma?

Saiba mais sobre a descoberta de dados no Microsoft Purview em **Microsoft.com**.

O desafio só tende a aumentar. Espera-se que a quantidade de novos dados criados, capturados, replicados e consumidos seja mais do que o dobro até 2026, com os dados corporativos crescendo com o dobro de rapidez em relação aos dados do consumidor.[4]

A Inteligência Artificial (IA) e o Machine Learning (ML) podem ajudar, reconhecendo dados confidenciais – como endereços de email, dados de saúde, números de cartão de crédito ou propriedade intelectual – e classificando-os automaticamente. A IA e o ML também podem aumentar a precisão da classificação e revisar dados retroativamente. Esses processos de identificação podem abranger toda a propriedade de dados, preservando, coletando, analisando, revisando e exportando conteúdo em qualquer lugar que ele resida, em qualquer nuvem.



[4] "Worldwide IDC Global DataSphere Forecast, 2022–2026: Enterprise Organizations Driving Most of the Data Growth", John Rydning, IDC. Maio de 2022.

Etapa 2

Classificar dados

As classificações e as políticas precisam seguir os dados à medida que eles se movimentam.

Por exemplo, se um funcionário copiar números de cartão de crédito de um documento do Microsoft Word para o Excel, a classificação e as políticas deverão se aplicar automaticamente a ambos os documentos.

Deseja gerenciar e proteger melhor os dados confidenciais em todo o seu ambiente?

Saiba mais sobre a classificação e proteção de dados no Microsoft Purview em **Microsoft.com**.

A classificação de dados adequada ajuda você a determinar as políticas certas e a mitigação de riscos para garantir que diferentes tipos de dados não sejam usados de forma acidental ou intencional, ou sejam acessados sem autorização. A criptografia e as marcas-d'água podem proteger os dados ainda mais – estejam em repouso, em trânsito ou em uso.

Mas a classificação e as políticas precisam seguir os dados à medida que se movimentam pela organização. As políticas de rotulagem e proteção não podem ser restritas a documentos separados; elas precisam se estender por toda a propriedade digital – de repositórios na infraestrutura local a repositórios baseados na nuvem, de SaaS (software como serviço) a aplicativos nativos do sistema operacional.

As abordagens tradicionais de classificação envolvem um trabalho manual considerável, que corre o risco de ter erros ou inadvertidamente negligenciar dados críticos. Os classificadores integrados e treináveis podem ajudar a automatizar esse processo, e uma solução integrada permite que os administradores gerenciem políticas centralmente, em todos os sistemas.

Etapa 3

Evite a perda de dados

A política de DLP pode impedir ações fora de conformidade.

Por exemplo, se um funcionário tentar fazer o download de uma planilha com números de cartão de crédito em um pen drive ou enviá-la para o armazenamento em nuvem, a política de DLP poderá identificar a atividade como fora de conformidade e evitá-la.

Deseja detecção inteligente e controle de informações confidenciais?

Saiba mais sobre a prevenção contra perda de dados no Microsoft Purview em **Microsoft.com**.

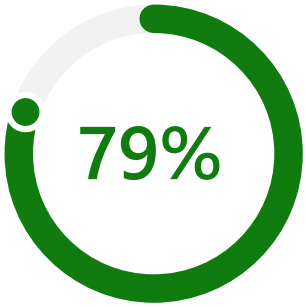
Depois que você identificar e classificar seus dados, as soluções de prevenção contra perda de dados (DLP) poderão aplicar políticas de proteção de ponta a ponta que atenuem ameaças como dados e exfiltração de dados incompreensíveis, de modo que os funcionários atuais e antigos não, intencionalmente ou inadvertidamente, compartilhem, exponham ou transfiram dados confidenciais sem autorização.

As soluções inteligentes de DLP usam o contexto para encontrar um equilíbrio entre fornecer flexibilidade e bloquear ações de alto risco. Por exemplo, os indivíduos podem ser capazes de continuar com uma ação depois de serem lembrados sobre os riscos potenciais e as políticas aplicáveis. Isso pode ajudar a proteger dados confidenciais e também treinar os usuários para entender melhor o risco.

As soluções de DLP ajudam a proteger a propriedade intelectual e outros dados de negócios críticos, melhorando também a conformidade com regulamentos como o GDPR (regulamento geral sobre a proteção de dados), a HIPAA (lei de portabilidade e prestação de informações de saúde) e a CCPA (lei de privacidade do consumidor da Califórnia).

Uma abordagem abrangente da DLP impõe políticas em toda a organização de forma consistente, protegendo os pontos do "elo mais fraco" no ciclo de vida dos dados.

Não anexe a proteção de dados. Integre-a.



Uma pesquisa com tomadores de decisão de conformidade mostrou que 79% tinham adquirido vários produtos de conformidade e proteção de dados.

A maioria tinha comprado três ou mais.[5]

Muitas organizações tentaram uma abordagem "anexar" de proteção de informações, usando várias soluções para gerenciar partes distintas do ciclo de vida dos dados. Mas isso força sua segurança, governança de dados, conformidade e equipes jurídicas a costurar uma manta de retalhos que, muitas vezes, é ineficaz e drena recursos.

Uma abordagem "integrada" pode fechar as lacunas, reunindo identificação de dados, classificação de dados e DLP. Com uma solução integrada, é mais fácil gerenciar e aplicar políticas centralmente. Isso também reduz o tempo de treinamento para os usuários, que recebem notificações de política de uma forma familiar, nativamente dentro de aplicações.

[5] "Pesquisa de fevereiro de 2022 com 200 tomadores e decisão dos-EUA (n=100 599-999 funcionários, n=100 1000+ funcionários) patrocinada pela Microsoft e feita pela MDC Research."

Uma solução interna e integrada: Microsoft Purview

O Microsoft Purview ajuda você a enfrentar os desafios do local de trabalho descentralizado e rico em dados de hoje, com um conjunto abrangente de soluções que ajudam você a governar, proteger e gerenciar toda a sua propriedade de dados.

Vá além da governança.

Saiba mais sobre como proteger seus dados com o Microsoft Purview >

Interessado em uma área específica de proteção de dados? Obtenha informações mais detalhadas sobre como o Microsoft Purview podem ajudar você com a:

Descoberta de dados >

Classificação e proteção de dados >

Prevenção contra perda de dados >

Microsoft Security