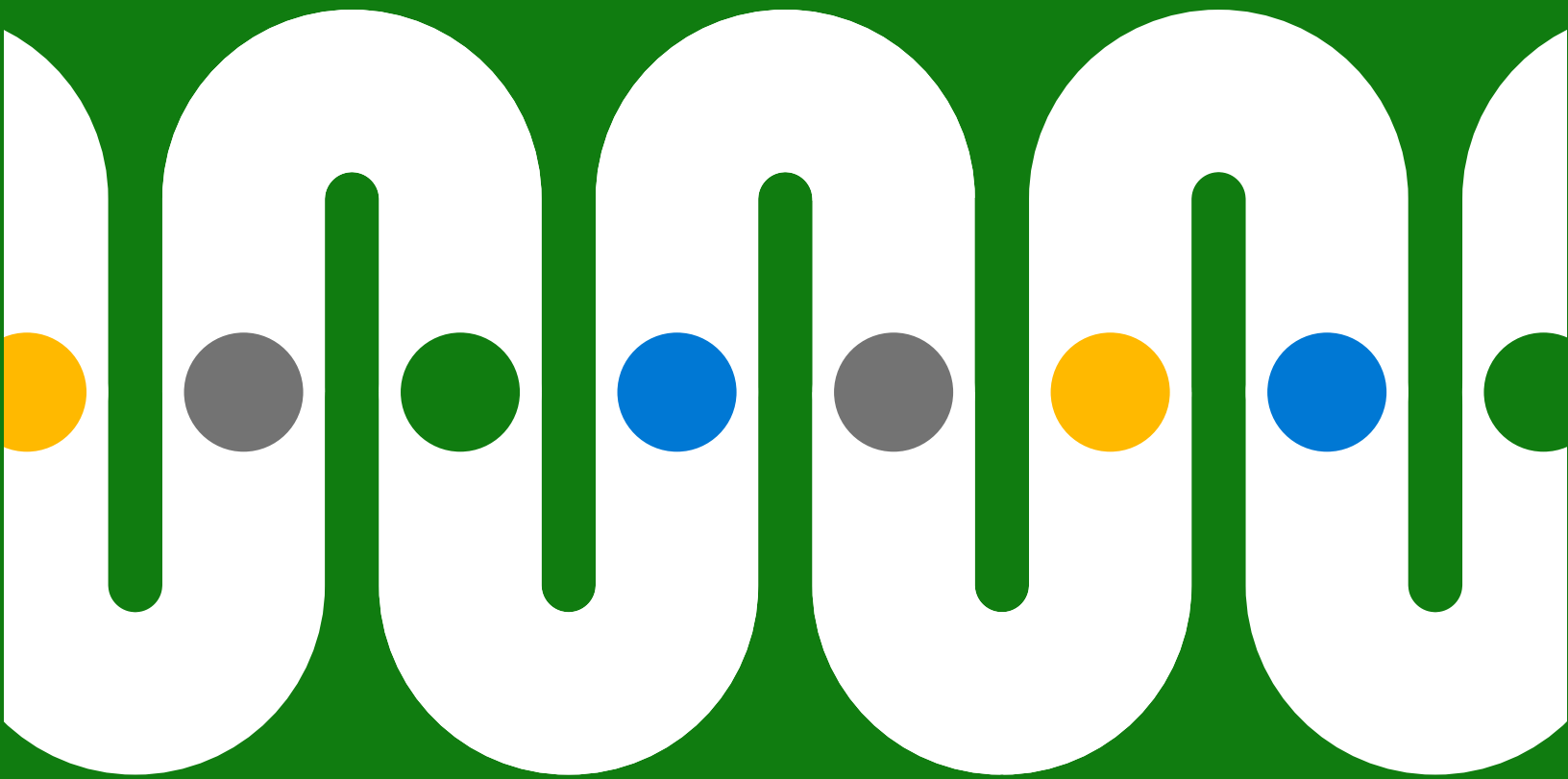
Microsoft Security

3 Passos para Proteger os seus Dados de Ponta a Ponta



Índice

Um inquérito aos decisores de conformidade revelou que 95% estavam preocupados com os desafios de proteção de dados.[2]

Introdução

As organizações verificaram um enorme aumento na sua pegada digital com o trabalho híbrido, que vai muito para além do escritório tradicional.

Esta situação levou a uma maior fragmentação e transferência de dados não autorizada, agravada pelo rápido crescimento de uma série de aplicações, dispositivos e localizações. A acrescentar a isto, muitos trabalhadores mudaram de funções em busca de maior satisfação ou flexibilidade, criando novos ângulos mortos em acervos de dados cada vez maiores.[1]

Todos estes fatores levaram os CIO e CISO a repensar a abordagem à proteção das informações. Num inquérito de acompanhamento a mais de 500 decisores de conformidade dos EUA, quase todos (95%) manifestaram preocupação com os desafios de proteção de dados.[2]

[1] "Como a Microsoft pode ajudar a reduzir o risco interno durante a Grande Remodelação, Alym Rayani", Microsoft Security. 28 de fevereiro de 2022.

[2] "Inquérito de setembro de 2021 a 512 decisores de conformidade dos EUA encomendado pela Microsoft à Vital Findings".

As equipas de TI e de segurança procuram melhores formas de gerir todo o ciclo de vida dos dados nos ambientes multicloud, na cloud híbrida e on-premises. Esta abordagem de ponta a ponta envolve três passos-chave:

Passo 1: Identificar os dados

Determine onde residem os seus dados, de que tipo são e como estão a ser utilizados ou partilhados

Passo 2: Classificar os dados

Classifique e identifique os dados para saber quais as políticas corretas e a mitigação de riscos a aplicar

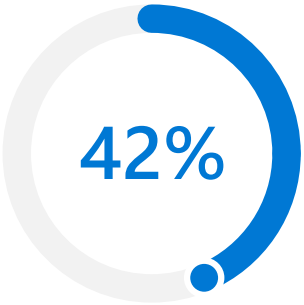
Passo 3: Evitar a perda de dados

Encontre um equilíbrio entre a redução de riscos e a flexibilidade para os seus colaboradores com deteção e controlo inteligentes

O objetivo desta abordagem? Colmatar as lacunas e minimizar o risco sem sacrificar a produtividade.

Passo 1

Identificar os dados



42% das organizações afirmaram que, pelo menos, metade dos respetivos dados eram "dark data".[3]

Estes dados "ocultos" podem assumir várias formas: desde anexos de e-mail e registos de chamadas de clientes a registos de computador e gravações de vídeo.

Se não conseguir identificar os dados, ou seja, saber onde residem, de que tipo são e como estão a ser utilizados ou partilhados, é impossível aplicar-lhes as políticas ou a proteção corretas.

As organizações modernas geram continuamente grandes quantidades de dados. Não se trata apenas documentos, e-mails e mensagens, mas tudo, desde filmagens de segurança a dados de geolocalização. Tudo isto agravado pela proliferação dos mesmos em aplicações, dispositivos e armazenamento, na infraestrutura on-premises e na cloud.

A identificação de todos estes dados pode ser difícil, e 42% das organizações dizem que pelo menos metade dos seus dados são "dark data".[3] Ou seja, informações recolhidas, mas desconhecidas ou não utilizadas para fins comerciais. Por vezes, tornam-se "dark data" quando o trabalhador que os criou muda de projeto ou função. Muitas vezes, simplesmente não estão instalados sistemas que identifiquem os dados no momento da sua criação ou modificação.

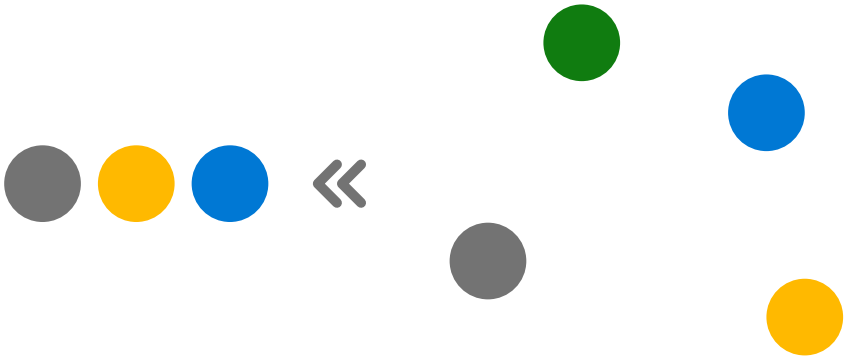
[3] "2022 State of Data Governance and Empowerment Report", Enterprise Strategy Group. Julho de 2022.

Quer criar um workflow de deteção de ponta a ponta numa única plataforma?

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

Este desafio só irá aumentar. Prevê-se que a quantidade de novos dados criados, capturados, replicados e consumidos aumente em mais do dobro até 2026, com os dados empresariais a crescer com o dobro da rapidez em relação aos dados do consumidor.[4]

A inteligência artificial (IA) e o machine learning (ML) podem ajudar ao reconhecer os dados confidenciais (como endereços de e-mail, dados de saúde, números de cartões de crédito ou propriedade intelectual) e ao classificá-los automaticamente. A IA e o ML também podem aumentar a precisão da classificação e analisar retroativamente dados. Estes processos de identificação podem abranger todo o seu acervo de dados e, deste modo, preservar, recolher, analisar, rever e exportar conteúdos onde quer que residam, em qualquer cloud.



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

Passo 2

Classificar os dados

As classificações e as políticas também têm de se aplicar aos dados à medida que estes circulam.

Por exemplo, se um colaborador de marketing copia números de cartões de crédito de um documento Microsoft Word para o Excel, a classificação e as políticas devem aplicar-se automaticamente a ambos os documentos.

Quer gerir e proteger melhor os dados confidenciais no seu ambiente?

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

Uma classificação de dados adequada ajuda a determinar as políticas corretas e a mitigação de riscos para assegurar que diferentes tipos de dados não são utilizados de forma acidental ou intencional, ou sem autorização. A encriptação e marcas d'água podem proteger ainda mais os dados, estejam eles em repouso, trânsito ou utilização.

Contudo, a classificação e as políticas também se devem aplicar aos dados à medida que estes circulam pela organização. As políticas de identificação e proteção não se podem limitar a documentos discretos, têm de abranger todo o património digital, desde repositórios on-premises a repositórios baseados na cloud, desde software como serviço (SaaS) a aplicações nativas de SO.

As abordagens de classificação tradicionais envolvem um trabalho manual considerável para classificar todos estes dados, correndo o risco de erros ou de ignorar inadvertidamente os dados críticos. Os classificadores integrados e passíveis de serem formados podem ajudar a automatizar este processo, e uma solução integrada permite aos administradores gerir políticas centralmente, em todos os sistemas.

Passo 3

Evitar a perda de dados

A política de DLP pode evitar ações que não estejam em conformidade.

Por exemplo, se um colaborador tentar fazer download de uma folha de cálculo com números de cartões de crédito para uma pen USB ou carregála para o armazenamento na cloud, a política de DLP pode identificar a atividade como não estando em conformidade e evitá-la.

Quer deteção inteligente e controlo de informações confidenciais?

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

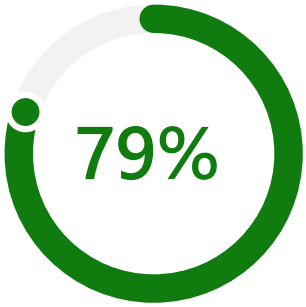
Após a identificação e classificação dos dados, as soluções de prevenção de perda de dados (DLP) podem impor políticas de proteção de ponta a ponta que mitiguem as ameaças, como as associadas a "dark data" e a transferências de dados não autorizadas. O objetivo é impedir que os colaboradores atuais e antigos partilhem, exponham ou transfiram dados confidenciais sem autorização, seja de forma intencional ou inadvertida.

As soluções inteligentes de DLP utilizam o contexto para encontrar um equilíbrio entre o fornecimento de flexibilidade de escolha e o bloqueio de ações de alto risco. Por exemplo, os indivíduos poderão prosseguir com uma ação depois de serem lembrados sobre os riscos potenciais e as políticas aplicáveis. Isto pode ajudar a proteger os dados confidenciais, ao mesmo tempo que vai formando os utilizadores no sentido de compreenderem melhor o risco.

As soluções de DLP ajudam a proteger a propriedade intelectual e outros dados empresariais críticos, melhorando também a conformidade com os regulamentos, como o Regulamento Geral sobre a Proteção de Dados (RGPD), a Lei de Responsabilização e Portabilidade de Informações de Saúde (HIPAA), e a Lei de Privacidade dos Consumidores da Califórnia (CCPA).

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

Escolha uma abordagem integrada à proteção de dados, e não acessória.



Um inquérito a decisores de conformidade revelou que 79% tinham adquirido vários produtos de conformidade e proteção de dados.

A maioria tinha adquirido três ou mais produtos.[5]

Muitas organizações experimentaram uma abordagem acessória à proteção das informações, utilizando várias soluções para gerir partes discretas do ciclo de vida dos dados. Contudo, isto obriga as equipas jurídicas, de segurança, de gestão de dados e de conformidade a reunir uma diversidade de ferramentas que é muitas vezes ineficaz e coloca os recursos sob pressão.

Uma abordagem integrada pode colmatar as lacunas, reunindo a identificação e classificação de dados, e a DLP. Com uma solução integrada, é mais fácil gerir e impor políticas centralmente. Também reduz o tempo de formação dos utilizadores, que recebem notificações de políticas de uma forma familiar e nativa dentro das aplicações.

[5] "Inquérito de fevereiro de 2022 a 200 decisores de conformidade dos EUA (n=100 599-999 colaboradores, n=100, mais de 1000 colaboradores) encomendado pela Microsoft à MDC Research."

Uma solução integrada: Microsoft Purview

O Microsoft Purview ajuda a enfrentar os desafios do atual local de trabalho descentralizado e rico em dados, com um conjunto abrangente de soluções que permitem administrar, proteger e gerir todo o seu acervo de dados.

Vá além da governação.

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

Tem interesse numa área específica de proteção de dados? Obtenha informações mais detalhadas sobre como Microsoft Purview pode ajudar com a:

Deteção de dados >

Classificação e proteção de dados >

Prevenção de perda de dados >

Microsoft Security