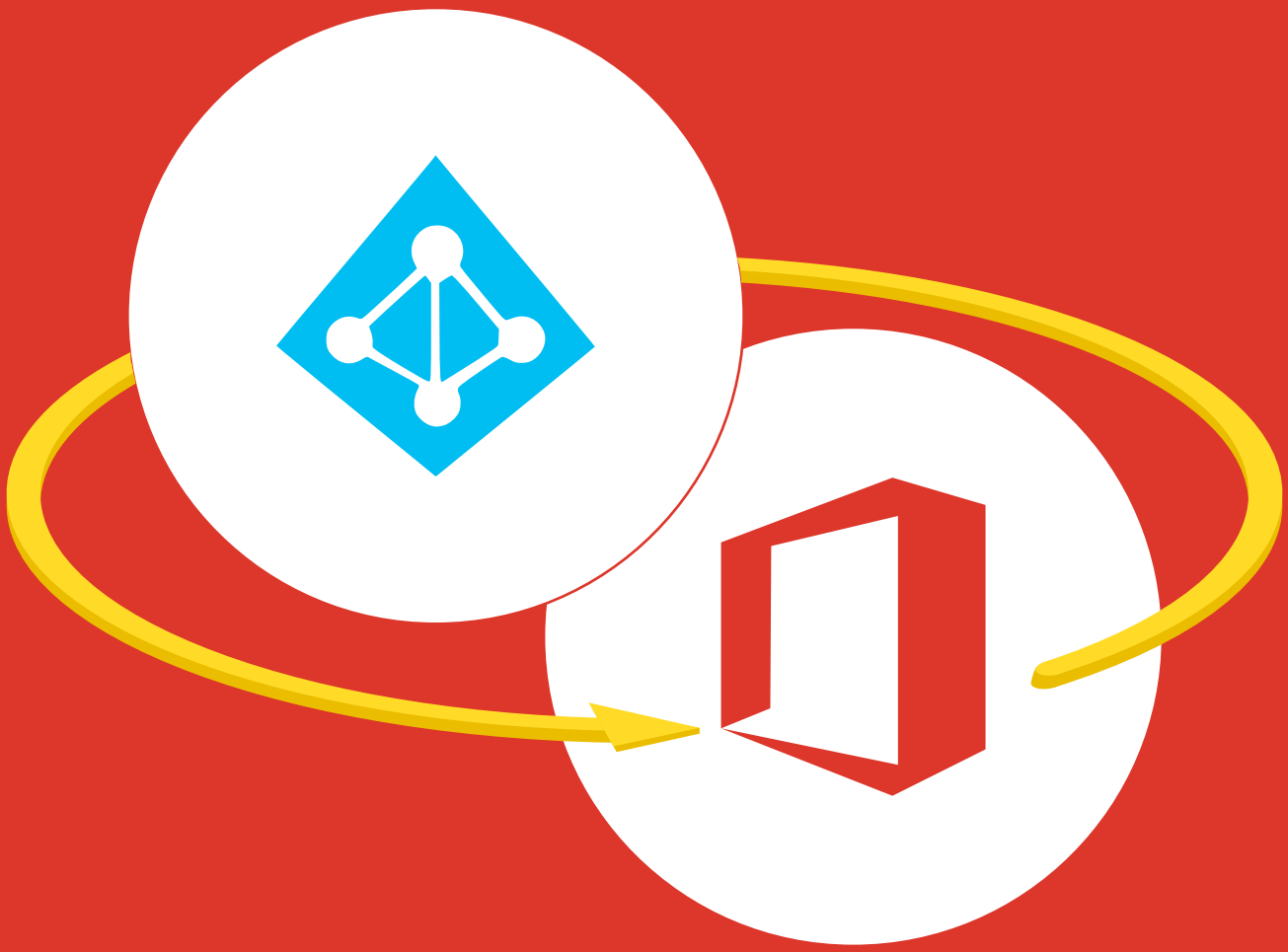
5 motivos

pelos quais você precisa de uma solução de proteção de dados corporativos



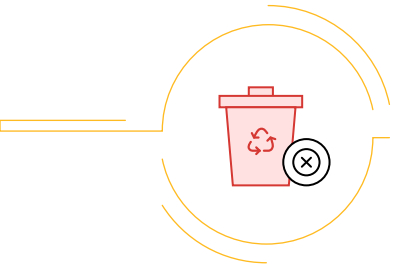
ManageEngine
RecoveryManager Plus

Introdução

A proteção de dados é, sem dúvida, a configuração de segurança cibernética mais importante no mundo da administração de TI. No entanto, na maioria das vezes, a ela fica em segundo plano no planejamento da postura de segurança cibernética. Por quê? Essa desconexão ocorre porque a maioria de nós não entende os reais benefícios de ter uma solução de proteção de dados eficaz.

Este guia explorará os motivos pelos quais você precisa de uma solução de proteção de dados para dados do Azure AD e do Microsoft 365 e como ela pode ajudar a prevenir a perda de dados em caso de interrupção.

Motivos para usar uma solução de proteção de dados empresariais



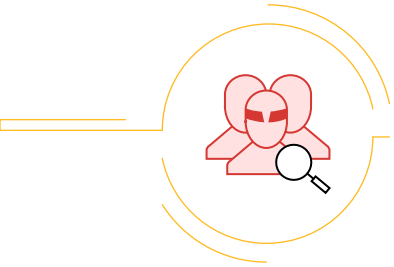
1. Exclusão acidental

A Microsoft mantém seus dados seguros armazenando-os em vários locais físicos, caso um deles falhe. No entanto, esse recurso também faz com que qualquer exclusão seja replicada em todas as outras localizações geográficas, e os dados excluídos serão removidos de todos os data centers.

A Microsoft fornece uma Lixeira de Reciclagem para seus serviços Azure AD, Exchange Online, SharePoint Online e OneDrive for Business, o que é útil para recuperar itens de exclusões acidentais. No entanto, há uma ressalva: a Lixeira tem um período limitado dentro do qual você pode restaurar itens excluídos.

- Itens excluídos do Azure AD são armazenados na Lixeira por no máximo 30 dias.
- Itens excluídos do Exchange Online são armazenados na Lixeira por no máximo 30 dias (120 dias para entradas de calendário).
- Arquivos e pastas excluídos do SharePoint Online e do OneDrive for Business são armazenados na Lixeira por no máximo 93 dias.
- Após o término do período de retenção, os itens excluídos não poderão ser recuperados.

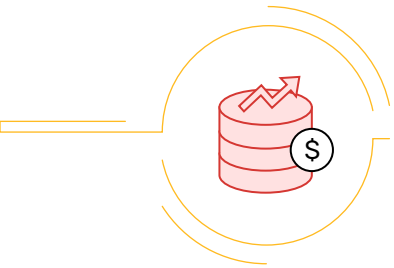
Por outro lado, uma solução de proteção de dados oferece a flexibilidade de fazer backup dos seus dados do Microsoft 365 e armazená-los indefinidamente até que você precise deles.



2. Ameaças internas

Dados críticos excluídos ou modificados por um administrador desonesto ou alguém se passando por administrador podem impactar negativamente uma organização se os dados não forem recuperados instantaneamente. Como a lixeira nativa vem com um temporizador, se você não notar que os itens foram excluídos a tempo, não poderá restaurá-los posteriormente, quando descobrir que foram excluídos.

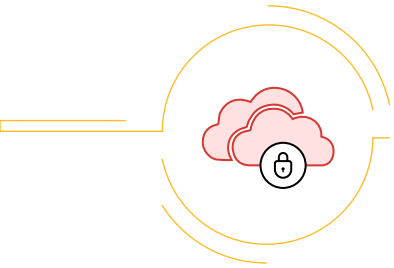
Ter uma solução de proteção de dados que faça backup frequente dos seus dados não apenas protege você de ataques maliciosos de terceiros, mas também o protege contra ações realizadas por seus próprios funcionários, intencionais ou não. Você pode reduzir o objetivo do ponto de recuperação do seu ambiente do Azure AD e do Microsoft 365 e parar de se preocupar com credenciais perdidas ou funcionários desonestos.



3. Aumento do custo de armazenamento adicional

Armazenar todos os dados do Microsoft 365 aumenta o tamanho do seu e-mail do Exchange Online e dos sites do OneDrive for Business ao longo do tempo. Quando os dados em seu e-mail e sites excedem o limite de armazenamento do seu plano, você terá que fazer upgrade para um plano com mais armazenamento, o que pode aumentar os custos rapidamente.

Com uma solução de proteção de dados, você sempre terá uma cópia de todos os seus dados e poderá restaurá-los em um piscar de olhos, eliminando a necessidade de pagar por planos de assinatura mais altos. Você pode manter e-mails e sites enxutos e restaurar os dados conforme e quando necessário.



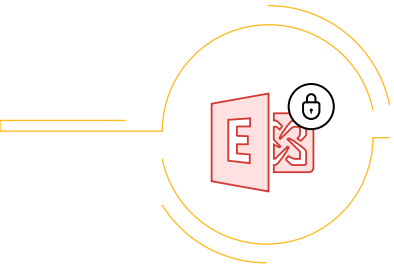
4. Entrada de ransomware e malware via cliente de sincronização do OneDrive

O cliente de sincronização do OneDrive da Microsoft é uma ferramenta que pode sincronizar seus dados do OneDrive da nuvem para o seu desktop e vice-versa. Embora essa ferramenta ofereça aos funcionários a flexibilidade de trabalhar de qualquer lugar e a qualquer hora, há uma grande vulnerabilidade que representa uma ameaça de ransomware.

Se um ataque de ransomware ao seu sistema infectar os arquivos na sua cópia sincronizada do OneDrive for Business, os dados serão sincronizados de volta para a nuvem e todos os dados no seu ambiente OneDrive for Business também serão infectados. Embora a Microsoft forneça uma maneira de detectar ransomware e se recuperar dele, ela também lista algumas limitações desse recurso.

- A Restauração de Arquivos usa o histórico de versões e a Lixeira para restaurar o OneDrive, portanto, está sujeita às mesmas restrições desses recursos. Quando o histórico de versões está desativado, a Restauração de Arquivos não consegue restaurar arquivos para uma versão anterior.
- Arquivos excluídos não podem ser restaurados após serem removidos da Lixeira do conjunto de sites — nem por exclusão manual nem esvaziando a Lixeira.
- Álbuns não são restaurados.
- Se você carregar um arquivo ou pasta novamente após excluí-lo, a Restauração de Arquivos ignorará a operação de restauração para esse arquivo ou pasta.

Ter uma solução de proteção de dados elimina todas essas limitações e permite que você se recupere facilmente de qualquer ataque de ransomware.



5. Ataques de ransomware em e-mails do Exchange Online

A maioria de nós está familiarizado com ataques de ransomware em documentos, mas ataques de ransomware em e-mails são novidade no setor. De acordo com o Relatório Anual de Ransomware da Datto, dos mais de 2.400 MSPs pesquisados, 28% afirmam ter presenciado ataques de ransomware em aplicações SaaS. Destes, quase metade dos entrevistados relatou ter visto ataques especificamente no Microsoft 365, com 22% relatando ataques ao G Suite. Esses ataques variam de ataques comuns de ransomware, sincronizados com aplicações em nuvem, até infecções mais sinistras, criadas especificamente para a nuvem.

Por esse motivo, ter a capacidade de recuperar todos os seus e-mails do Microsoft 365 de uma só vez é algo essencial para toda organização.