6 motivos para fazer backup do Microsoft Entra ID

Introdução

O Microsoft Entra ID (anteriormente conhecido como Azure Active Directory) é essencial para o gerenciamento moderno de identidade e acesso (IAM). No entanto, sua importância também o torna um dos principais alvos dos cibercriminosos. Com 600 milhões de ataques direcionados ao Microsoft Entra ID todos os dias, os riscos têm se tornado cada vez mais complexos e prejudiciais, representando desafios significativos para organizações em todo o mundo.

As ameaças são tão variadas quanto perigosas. Desde golpes de phishing que induzem os usuários a entregar credenciais até ataques de preenchimento de credenciais que exploram dados roubados, os agentes de ameaças são implacáveis. As consequências são catastróficas:

- Os funcionários perdem acesso a sistemas críticos, paralisando a produtividade.
- Os clientes não conseguem acessar os serviços, o que gera frustração e rotatividade em potencial.
- O tempo de inatividade e os esforços de recuperação drenam recursos, enquanto as multas regulatórias aumentam o fardo.
- A notícia de uma violação se espalha rapidamente, minando a confiança com clientes, parceiros e partes interessadas.
- Violações de dados muitas vezes levam a violações de regulamentos como GDPR ou HIPAA, resultando em penalidades pesadas.

Recuperar-se de um ataque não é pouca coisa. Isso demanda tempo, recursos e uma estratégia clara para restaurar as operações e reconstruir a confiança. E embora a Microsoft ofereça recursos robustos de segurança, é das empresas o ônus de proteger seus dados de acordo com o modelo de responsabilidade compartilhada. As ameaças de segurança são apenas uma das razões pelas quais você precisa proteger os dados do Microsoft Entra ID, e este e-book revelará e explicará muito mais.

1

Ameaças à segurança

O risco sempre presente de ataques virtuais exige defesas robustas para proteção contra acesso não autorizado e possíveis violações.

2

Conformidade

Práticas adequadas de gerenciamento de dados garantem a conformidade com padrões locais, nacionais e globais.

3

Exclusões acidentais e configurações incorretas

O erro humano pode levar à enorme perda de dados e a interrupções significativas.

4

Limitações da lixeira

A dependência de ferramentas integradas como a Lixeira é insuficiente para uma recuperação completa dos dados.

5

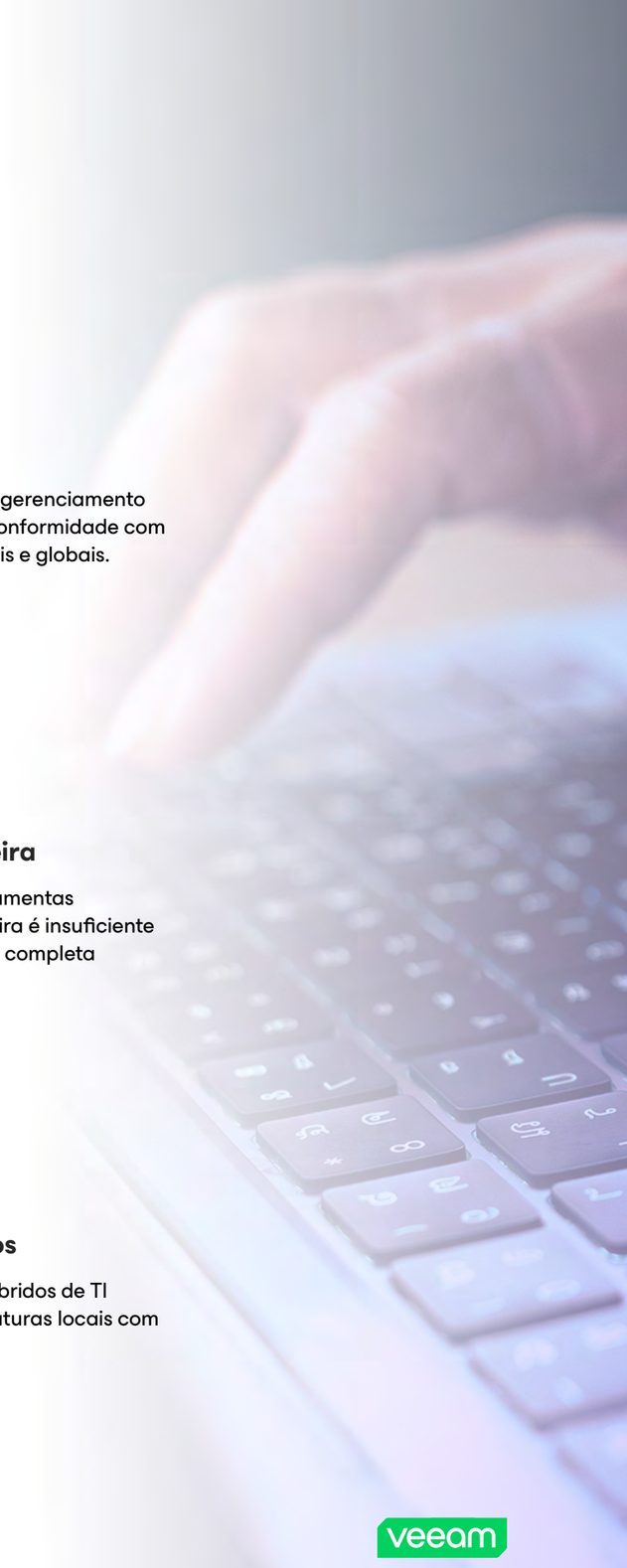
Recuperação eficiente

Minimizar o tempo de inatividade e garantir uma recuperação rápida de incidentes de perda de dados são vitais para manter as operações de negócios.

6

Ambientes híbridos

Gerenciar ambientes híbridos de TI exige integrar infraestruturas locais com soluções em nuvem.



1. Ameaças à segurança

O Microsoft Entra ID é parte integrante do gerenciamento de identidade e acesso (IAM) no Microsoft 365, Azure e várias outras plataformas. Muitas vezes despercebido pelos usuários, seu uso é crucial toda vez que eles fazem login. No entanto, é justamente essa invisibilidade que faz do Microsoft Entra ID um alvo preferencial para os cibercriminosos.

Os agentes de ameaças estão constantemente evoluindo suas táticas, e eles só precisam ter sucesso uma vez, enquanto os defensores devem ser perfeitos sempre. Os invasores são hábeis, empregando táticas como phishing e preenchimento de credenciais, onde senhas roubadas são usadas para violar contas. O ransomware, embora diferente, é igualmente disruptivo, bloqueando as empresas de seus ambientes de nuvem e interrompendo as operações.

Em um mundo ideal, as organizações optariam por evitar que violações ocorram em primeiro lugar. Muitas estratégias de mitigação de riscos são muito eficazes, e recursos como monitoramento proativo e ferramentas de análise de ameaças ajudam imensamente.

No entanto, nenhuma defesa é infalível. É aqui que o backup e a recuperação se tornam essenciais. Uma estratégia de backup robusta garante que, mesmo se os invasores violarem as suas defesas, você poderá restaurar rapidamente o acesso a dados essenciais de identidade. Seja para se recuperar de um ransomware, reverter exclusões acidentais ou mitigar ameaças internas, os backups funcionam como a sua rede de proteção.

Para o Microsoft Entra ID, redundância não significa exagero, significa sobrevivência. Quando os dados de identidade passam por backup e são facilmente recuperáveis, as empresas se protegem contra os efeitos incapacitantes da perda desses dados.

2. Conformidade

A conformidade normativa é imprescindível para a maioria das empresas, já que leis como GDPR e HIPAA exigem adesão estrita à privacidade, segurança e transparência dos dados. As apostas são altas: O não cumprimento pode resultar em multas de até 4% da receita anual ou 20 milhões de euros, o que for maior.

No contexto do Microsoft Entra ID, a conformidade está diretamente ligada ao gerenciamento eficaz das permissões de usuários e grupos. Configurações incorretas ou alterações não autorizadas podem expor dados confidenciais, levando a brechas e violações de conformidade. Por exemplo, se um administrador acidentalmente conceder permissões excessivas ou excluir um grupo de usuários crítico, os dados confidenciais poderão cair em mãos erradas e os reguladores não hesitarão em agir.

Para manter a conformidade, as organizações precisam de controles de segurança robustos, incluindo criptografia, gerenciamento de acesso e registros de auditoria. Mas uma das ferramentas mais essenciais em seu kit de ferramentas de conformidade é uma solução de backup abrangente.

Os backups garantem que seus dados do Microsoft Entra ID estejam sempre seguros, recuperáveis e alinhados com os padrões regulatórios. Se ocorrer uma configuração incorreta ou alteração não autorizada, você pode detectar isso rapidamente e restaurar as configurações corretas, minimizando o risco de não conformidade e exposição de dados.

3. Exclusões acidentais e configurações incorretas

Imagine se um administrador excluísse acidentalmente um grupo de usuários críticos ou configurasse incorretamente os controles de acesso no Microsoft Entra ID. De repente, usuários legítimos são bloqueados de sistemas essenciais, ou pior, usuários não autorizados ganham acesso. Em um sistema tão central como o Microsoft Entra ID, mesmo um pequeno erro pode ter consequências de longo alcance.

As repercussões desses erros de configuração e exclusões são profundas. Eles podem tornar sistemas críticos inacessíveis, causando tempo de inatividade operacional, perdas de produtividade e processos de recuperação dispendiosos. Além disso, esses erros podem prejudicar a confiança que clientes e parceiros depositam em uma organização, potencialmente afetando relacionamentos comerciais de longo prazo.

Mas aqui está a boa notícia: Uma solução de backup abrangente pode transformar um desastre em um pequeno soluço. Com os backups, exclusões acidentais ou erros de configuração podem ser corrigidos em minutos. Seja restaurando um grupo de usuários excluído ou revertendo para uma configuração segura anterior a erros, os backups adequados garantem que os erros não se transformem em crises.

Erros acontecerão; é da natureza humana. Mas com uma estratégia de backup robusta, suas consequências são mais evitáveis do que nunca.

4. Limitações da lixeira

Além de seu cronograma de retenção curto, a Lixeira nativa do Microsoft Entra ID tem escopo limitado. Tipos de dados como Atribuições de Função e Políticas de Acesso Condicional não são retidos, tornando-se imediatamente inacessíveis após a exclusão, ou seja, sem segundas chances. As restrições quanto ao volume de dados recuperáveis também apresentam limitações. A Lixeira do Microsoft Entra ID é um recurso útil, mas está longe de ser uma solução completa. Embora ofereça uma janela de recuperação de até 30 dias para certos tipos de dados, isso é insuficiente em cenários do mundo real. De acordo com o Microsoft Defense Report 2024, o tempo médio de detecção de incidentes é de 207 dias, muito além do período de retenção da Lixeira. Quando você percebe que os dados estão faltando, muitas vezes é tarde demais para recuperar.

A história da lixeira é esta: Quando o período de retenção expirar ou se os dados escaparem da lixeira devido a exclusões manuais ou remoção permanente, a recuperação por meio das ferramentas nativas da Microsoft se torna impossível. Uma solução de backup dedicada é a única maneira de preencher essas lacunas e ir além das proteções integradas da Microsoft. Fornece uma rede de segurança confiável contra perda de dados acidental ou intencional e garante que quase todos os tipos de dados de identidade possam ser recuperados.

5. Recuperação eficiente

As violações nem sempre começam com um estrondo. Muitos começam com alterações pequenas e despercebidas: um ajuste não autorizado nas permissões, a exclusão de um grupo de segurança ou um pequeno ajuste nas configurações. A capacidade de detectar essas mudanças precocemente é vital para evitar que elas se transformem em ameaças sérias.

A chave para evitar esses problemas é a detecção acelerada de alterações. Os administradores devem ser capazes de antecipar e resolver problemas antes que eles precisem de uma resposta importante. Em conjunto, as opções de recuperação granular permitem que as organizações restaurem exatamente os objetos que são necessários, desde uma única conta de usuário até uma estrutura de diretório completa, de forma eficiente e sem induzir tempo de inatividade desnecessário.

Então, como é uma recuperação eficiente para o Microsoft Entra ID? É uma combinação de:

- **Comparação de metadados:** Antes de restaurar, compare as configurações de produção com os pontos de restauração do backup. Essa etapa garante que você identifique exatamente o que foi alterado, para poder restaurar apenas o que for necessário.
- **Restauração no nível do objeto:** Com recursos granulares de restauração no nível do objeto, você pode recuperar itens específicos sem interromper o restante do seu ambiente.
- **Backups regulares:** Garanta que todas as alterações e configurações sejam salvas de tempos em tempos em um provisionar seguro. Isso cria uma rede de segurança confiável, permitindo uma restauração rápida e precisa quando surgirem problemas.
- **Planos de recuperação acionáveis:** Forneça processos claros e passo a passo para restaurar sistemas, para que a sua empresa possa ter uma recuperação rápida, segura e perfeita.

Juntos, esses elementos formam uma estratégia de recuperação abrangente que minimiza o tempo de inatividade, reduz o risco e mantém o seu ambiente do Microsoft Entra ID seguro e acessível.

6. Ambientes híbridos

Gerenciar a identidade no Active Directory (AD) local e no Microsoft Entra ID em um ambiente híbrido traz flexibilidade e complexidade. Com os usuários sincronizando constantemente entre sistemas na nuvem e no local, exclusões acidentais, configurações erradas ou problemas de sincronização podem interromper o acesso e introduzir riscos à segurança. Quando um usuário é removido, intencionalmente ou por engano, a capacidade de restaurar não só sua identidade, mas também seus relacionamentos e permissões, é crucial para a continuidade dos negócios.

O Microsoft Entra Connect e outras ferramentas de sincronização se concentram em manter os dados de identidade consistentes entre o AD e o Entra ID, mas não são projetados para recuperação total. Quando um usuário sincronizado é excluído, o Entra Connect pode restaurá-lo sem suas funções, associações de grupo e licenças originais, forçando os administradores a reconstruir manualmente sua identidade. Esse processo é demorado e aumenta o risco de restaurações incompletas ou desalinhamento de privilégios.

O gerenciamento de identidades híbridas não se trata apenas de manter os usuários ativos, mas de restaurá-los com os acessos, funções e configurações de segurança corretos intactos. Sem uma estratégia de backup adequada, as equipes de TI podem passar horas corrigindo manualmente problemas de acesso após uma exclusão ou um erro de sincronização.

Veeam Data Cloud for Microsoft Entra ID

Os desafios para proteger o Microsoft Entra ID são claros: Erros humanos, ameaças virtuais e exigências de conformidade criam riscos constantes. Sem uma estratégia de backup resiliente, até mesmo um pequeno passo em falso pode levar a tempo de inatividade, perda de produtividade e falhas de segurança.

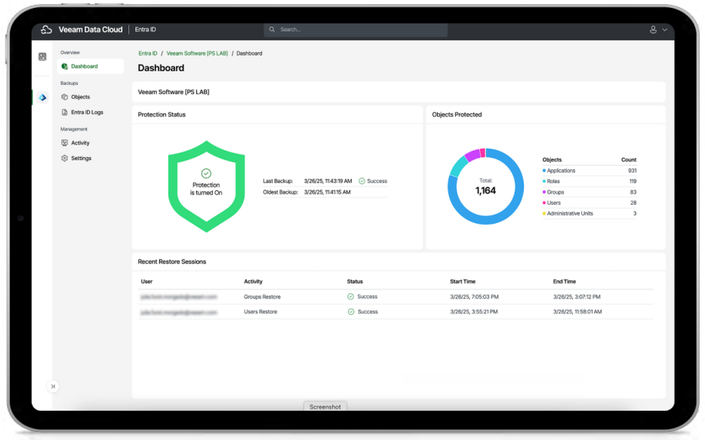
O Microsoft Entra ID é a espinha dorsal da identidade digital da sua organização e sua proteção é inegociável. Com o **Veeam Data Cloud for Microsoft Entra ID**, você pode simplificar a proteção de dados e garantir que sua infraestrutura de identidade permaneça segura, em conformidade e sempre disponível.

Essa solução de backup para SaaS oferece:

Backup e restauração abrangentes: Proteja usuários, grupos, inscrições de aplicativos e vários outros objetos

Armazenamento ilimitado: Escalone facilmente com storage ilimitado integrado à solução de backup SaaS

Experiência do usuário perfeita: Uma interface de usuário moderna e unificada, desenvolvida para facilitar o uso.



O Microsoft Entra ID é essencial demais para deixar desprotegido. Os riscos são reais, mas a solução também. A Veeam oferece a segurança, a resiliência e a tranquilidade de que as organizações modernas precisam para manter sua infraestrutura de identidade protegida, em conformidade e sempre disponível.

Solicite uma demonstração

Contato com vendas

Saiba mais sobre a proteção do Microsoft 365

Backup do Microsoft 365 e Entra ID juntos

Esse relatório vai mostrar:

- Qual é a responsabilidade da sua organização em relação ao Microsoft 365
- Por que proteger dados do Microsoft 365 é tão crucial hoje
- Como identificar lacunas na segurança de suas organizações
- As vantagens de utilizar um serviço de backup em comparação a outros métodos

→ 7 motivos críticos para fazer backup do Microsoft 365