6 raisons de sauvegarder Microsoft Entra ID

Introduction

Microsoft Entra ID (anciennement Azure Active Directory) joue un rôle essentiel dans la gestion moderne des identités et des accès (IAM). Cependant, son importance en fait également une cible de choix pour les cybercriminels. Avec plus de 600 millions d'attaques ciblant Microsoft Entra ID chaque jour, les risques sont devenus de plus en plus complexes et préjudiciables, posant des défis importants pour les entreprises du monde entier.

Les menaces sont aussi variées que dangereuses. Qu'il s'agisse d'escroqueries par hameçonnage qui incitent les utilisateurs à fournir des informations d'identification ou d'attaques par bourrage d'informations d'identification qui exploitent les données volées, les acteurs malveillants sont implacables. Les retombées sont catastrophiques :

- Les employés perdent l'accès à leurs systèmes critiques, ce qui paralyse la productivité.
- Les clients ne peuvent pas accéder aux services, ce qui entraîne de la frustration et une attrition des prospects.
- Les temps d'arrêt et les efforts de restauration épuisent les ressources, tandis que les amendes réglementaires alourdissent la charge.
- La nouvelle d'une violation se répand rapidement, érodant la confiance des clients, des partenaires et des parties prenantes.
- Les violations de données entraînent souvent des violations de réglementations telles que le RGPD ou HIPAA, entraînant de lourdes sanctions.

© 2025 Veeam Software. Tous droits réservés. Toutes les marques déposées sont la propriété de leurs détenteurs respectifs.

Effectuer une restauration après une attaque n'est pas chose aisée. Cela demande du temps, des ressources et une stratégie claire pour restaurer les opérations et rétablir la confiance. Et si Microsoft fournit des fonctionnalités de sécurité efficaces, il incombe aux entreprises de protéger leurs données selon un modèle de partage des responsabilités. Les menaces de sécurité ne sont qu'une des raisons pour lesquelles vous devez protéger les données Microsoft Entra ID, et cet e-book vous en dévoile et vous en explique bien d'autres.

© 2025 Veeam Software. Tous droits réservés. Toutes les marques déposées sont la propriété de leurs détenteurs respectifs.

1

Menaces à la sécurité

Le risque toujours présent de cyberattaques nécessite des défenses robustes pour se protéger contre les accès non autorisés et les violations potentielles.

2

Conformité

Des pratiques appropriées de gestion des données garantissent la conformité aux normes locales, nationales et mondiales.

3

Suppressions accidentelles et erreurs de configuration

L'erreur humaine peut provoquer des pertes de données considérables et des perturbations importantes.

4

Limites de la corbeille

Les outils intégrés, tels que la corbeille, ne suffisent pas à assurer une restauration complète des données.

5

Restauration efficace

Il est donc essentiel de minimiser les temps d'arrêt et d'assurer une restauration rapide après un incident entraînant des pertes de données pour assurer la continuité des activités.

6

Environnements hybrides

Pour faire face à la complexité des environnements IT hybrides, il faut s'adapter à la fois aux environnements locaux et aux environnements cloud.

veeam

1. Menaces à la sécurité

Microsoft Entra ID fait partie intégrante de la gestion des identités et des accès (IAM) dans Microsoft 365, Azure et de nombreuses autres plateformes. Souvent inaperçue des utilisateurs, son utilisation est cruciale à chaque fois qu'ils se connectent. Pourtant, c'est précisément cette invisibilité qui fait de Microsoft Entra ID une cible de choix pour les cybercriminels.

Les acteurs de la menace font constamment évoluer leurs tactiques, et ils n'ont besoin de réussir qu'une seule fois, tandis que les défenseurs doivent être parfaits à chaque fois. Les attaquants sont habiles et emploient des tactiques telles que le phishing et le credential stuffing, où les mots de passe volés sont utilisés pour pirater des comptes. Les ransomware, bien que différents, sont tout aussi perturbateurs : ils bloquent l'accès des entreprises à leurs environnements cloud et bloquent leurs opérations.

Dans un monde idéal, les entreprises choisiraient d'empêcher les violations de se produire en premier lieu. De nombreuses stratégies d'atténuation des risques sont très efficaces, et des ressources telles que des outils de supervision proactive et d'analyse des menaces se révèlent très utiles.

Cependant, aucune défense n'est infaillible. C'est là que la sauvegarde et la restauration deviennent essentielles. Une stratégie de sauvegarde efficace garantit que même si des attaquants franchissent vos défenses, vous pouvez rapidement restaurer l'accès à vos données d'identité stratégiques. Les sauvegardes sont votre filet de sécurité pour restaurer les données après une attaque par ransomware, annuler une suppression accidentelle ou atténuer les menaces internes.

Pour Microsoft Entra ID, la redondance n'est pas synonyme d'exagération, c'est une question de survie. Lorsque les données d'identité sont sauvegardées et peuvent être facilement restaurées, les entreprises se protègent contre les effets dévastateurs de leur perte.

© 2025 Veeam Software. Tous droits réservés. Toutes les marques déposées sont la propriété de leurs détenteurs respectifs.

2. Conformité

La conformité réglementaire est impérative pour la plupart des entreprises, car des lois telles que le RGPD et la loi HIPAA exigent le strict respect de la confidentialité, de la sécurité et de la transparence des données. L'enjeu est de taille : la non-conformité peut entraîner des amendes allant jusqu'à 4 % du chiffre d'affaires annuel ou 20 millions d'euros, selon le montant le plus élevé.

Dans le contexte de Microsoft Entra ID, la conformité dépend d'une bonne gestion des autorisations des utilisateurs et des groupes. Des erreurs de configuration ou des modifications non autorisées peuvent exposer des données sensibles, entraînant des violations de conformité. Par exemple, si un administrateur accorde accidentellement des autorisations excessives ou supprime un groupe d'utilisateurs critique, des données sensibles pourraient tomber entre de mauvaises mains, et les régulateurs n'hésiteront pas à agir.

Pour rester conformes, les entreprises ont besoin de contrôles de sécurité efficaces, y compris le chiffrement, la gestion des accès et la journalisation des audits. Mais l'un des outils les plus essentiels de votre kit de conformité est une solution de sauvegarde complète.

Grâce aux sauvegardes, vous avez l'assurance que vos données Microsoft Entra ID sont toujours sécurisées, récupérables et conformes aux normes réglementaires. En cas de mauvaise configuration ou de modification non autorisée, vous pouvez rapidement la détecter et restaurer les paramètres appropriés, réduisant ainsi le risque de non-conformité et d'exposition des données.

© 2025 Veeam Software. Tous droits réservés. Toutes les marques déposées sont la propriété de leurs détenteurs respectifs.

3. Suppressions accidentelles et erreurs de configuration

Imaginez qu'un administrateur supprime accidentellement un groupe d'utilisateurs critique ou configure mal les contrôles d'accès dans Microsoft Entra ID. Soudainement, des utilisateurs légitimes sont exclus des systèmes essentiels, ou pire, des utilisateurs non autorisés y accèdent. Dans un système aussi central que Microsoft Entra ID, même la plus petite erreur peut avoir des conséquences lourdes.

Les répercussions de ces erreurs de configuration et suppressions sont profondes. Elles peuvent rendre les systèmes stratégiques inaccessibles, entraînant des temps d'arrêt opérationnels, des pertes de productivité et des processus de restauration coûteux. De plus, ces erreurs peuvent compromettre la confiance que les clients et les partenaires accordent à une entreprise, ce qui peut affecter les relations commerciales à long terme.

Mais voici la bonne nouvelle : une solution de sauvegarde complète peut transformer un sinistre en un petit contretemps. Avec les sauvegardes, les suppressions accidentelles ou les erreurs de configuration peuvent être corrigées en quelques minutes. Qu'il s'agisse de restaurer un groupe d'utilisateurs supprimé ou de rétablir une configuration sécurisée antérieure à l'erreur, des sauvegardes appropriées permettent d'éviter que les erreurs ne se transforment en crises.

Des erreurs se produiront ; c'est la nature humaine. Mais avec une stratégie de sauvegarde efficace, leurs conséquences sont plus que jamais évitables.

© 2025 Veeam Software. Tous droits réservés. Toutes les marques déposées sont la propriété de leurs détenteurs respectifs.

4. Limites de la corbeille

Outre sa courte durée de rétention, la corbeille native de Microsoft Entra ID est limitée. Les types de données tels que les attributions de rôles et les stratégies d'accès conditionnel ne sont pas du tout conservés et deviennent immédiatement inaccessibles une fois la suppression terminée, ce qui signifie qu'il n'y a pas de seconde chance. Les contraintes qui pèsent sur le volume des données récupérables présentent également des limites. La corbeille de Microsoft Entra ID est une fonctionnalité utile, mais elle est loin d'être une solution complète. Alors qu'elle offre une fenêtre de restauration allant jusqu'à 30 jours pour certains types de données, elle reste insuffisante dans les scénarios réels. Selon le rapport Microsoft Defense Report 2024, le temps moyen de détection des incidents est de 207 jours, bien au-delà de la période de rétention de la corbeille. Lorsque vous vous rendez compte qu'il manque des données, il est souvent trop tard pour les restaurer.

Voici comment se déroule l'histoire de la corbeille : À la fin de la période de rétention, ou si les données ne sont pas stockées dans la corbeille en raison d'une suppression manuelle ou définitive, il devient impossible d'effectuer une restauration au moyen des outils natifs de Microsoft. Une solution de sauvegarde dédiée est le seul moyen de combler ces lacunes et d'aller au-delà des dispositifs de protection intégrés de Microsoft. Ce faisant, vous disposez d'un filet de sécurité fiable contre les pertes de données accidentelles ou intentionnelles et vous assurez que presque tous les types de données d'identité sont récupérables.

© 2025 Veeam Software. Tous droits réservés. Toutes les marques déposées sont la propriété de leurs détenteurs respectifs.

5. Restauration efficace

Les violations ne commencent pas toujours par un coup de tonnerre. Beaucoup commencent par de petits changements inaperçus : un ajustement non autorisé des autorisations, la suppression d'un groupe de sécurité ou une modification mineure des paramètres. La capacité de détecter ces changements à un stade précoce est essentielle pour éviter qu'ils ne se transforment en menaces sérieuses.

La clé pour éviter ces problèmes est la détection accélérée des changements. Les administrateurs doivent être capables d'anticiper et de résoudre les problèmes avant qu'ils ne nécessitent une réponse majeure. Grâce aux options de restauration granulaire, les entreprises sont habilitées à restaurer précisément les objets nécessaires, d'un simple compte utilisateur à une structure de répertoire complète, de manière efficace et sans engendrer de temps d'arrêt inutiles.

Alors, à quoi ressemble une restauration efficace pour Microsoft Entra ID ?
Ce processus associe :

- **Comparaison des métadonnées :** Avant toute restauration, comparez les configurations de production avec les points de restauration de sauvegarde. Cette étape vous permet d'identifier exactement ce qui a changé afin de ne restaurer que le nécessaire.
- **Restauration au niveau objet :** Les fonctionnalités de restauration granulaires au niveau des objets permettent de restaurer des objets spécifiques sans perturber le reste de votre environnement.
- **Sauvegardes régulières :** Assurez-vous que toutes les modifications et configurations sont enregistrées périodiquement dans sur une cible sécurisée. Cela crée un filet de sécurité fiable permettant une restauration rapide et précise en cas de problème.
- **Plans de restauration exploitables :** Définissez des processus clairs de restauration, étape par étape, afin que votre entreprise puisse effectuer une restauration rapide, sécurisée et transparente.

Ensemble, ces éléments forment une stratégie de restauration complète qui minimise les temps d'arrêt, réduit les risques et garantit la sécurité et l'accessibilité de votre environnement Microsoft Entra ID.

© 2025 Veeam Software. Tous droits réservés. Toutes les marques déposées sont la propriété de leurs détenteurs respectifs.

6. Environnements hybrides

La gestion des identités sur site Active Directory (AD) et Microsoft Entra ID dans un environnement hybride est à la fois flexible et complexe. Les utilisateurs effectuant une synchronisation constante entre le cloud et les systèmes sur site, les suppressions accidentelles, les erreurs de configuration ou les problèmes de synchronisation peuvent perturber l'accès et présenter des risques de sécurité. Lorsqu'un utilisateur est supprimé (intentionnellement ou par erreur), la capacité à restaurer non seulement son identité, mais aussi ses relations et ses autorisations est cruciale pour la continuité de l'activité.

Microsoft Entra Connect et d'autres outils de synchronisation se concentrent sur le maintien de la cohérence des données d'identité entre AD et Entra ID, mais ils ne sont pas conçus pour une restauration complète. Lorsqu'un utilisateur synchronisé est supprimé, Entra Connect peut le restaurer sans ses rôles, appartenances à des groupes et licences d'origine, ce qui oblige les administrateurs à reconstruire manuellement son identité. Cette procédure prend du temps et augmente le risque de restaurations incomplètes ou de désalignement des privilèges.

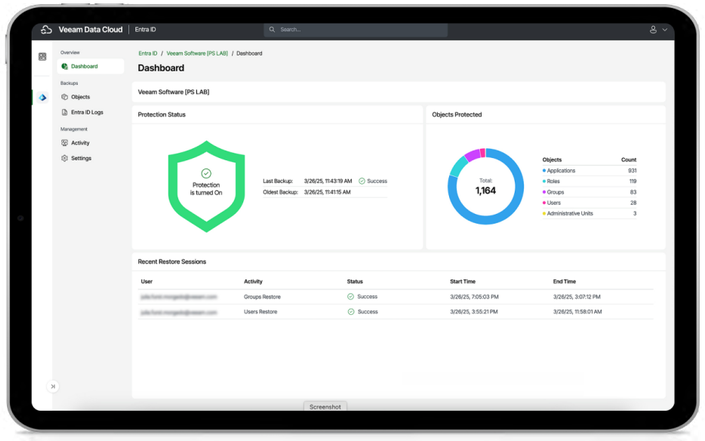
La gestion des identités hybrides ne consiste pas seulement à maintenir les utilisateurs actifs, il s'agit de les restaurer avec les bons accès et rôles et les paramètres de sécurité intacts. Sans stratégie de sauvegarde appropriée, les équipes informatiques peuvent passer des heures à corriger manuellement les problèmes d'accès après une suppression ou un incident de synchronisation.

© 2025 Veeam Software. Tous droits réservés. Toutes les marques déposées sont la propriété de leurs détenteurs respectifs.

Veeam Data Cloud for Microsoft Entra ID

Les défis liés à la sécurisation de Microsoft Entra ID sont clairs : l'erreur humaine, les cybermenaces et les exigences de conformité engendrent des risques constants. Sans une stratégie de sauvegarde résiliente, le moindre faux pas peut entraîner des temps d'arrêt, des pertes de productivité et des failles de sécurité.

Microsoft Entra ID est l'épine dorsale de l'identité numérique de votre organisation, et sa protection n'est pas négociable. Avec **Veeam Data Cloud pour Microsoft Entra ID,** vous simplifiez la protection des données et vous vous assurez que votre infrastructure d'identité reste sécurisée, conforme et toujours disponible.



Cette solution de sauvegarde SaaS offre :

Sauvegarde et restauration complètes : Protégez les utilisateurs, les groupes, les inscriptions d'applications et plusieurs autres objets.

Stockage illimité : Bénéficiez d'une évolutivité sans effort grâce au stockage illimité intégré à la solution de sauvegarde SaaS.

Expérience utilisateur transparente : Une interface utilisateur moderne et unifiée conçue pour une utilisation facile.

Microsoft Entra ID est trop critique pour être laissé sans protection. Les risques sont réels, mais la solution l'est tout autant. Veeam offre la sécurité, la résilience et la tranquillité d'esprit dont ont besoin les entreprises modernes pour assurer la protection, la conformité et la disponibilité permanentes de leur infrastructure de gestion des identités.

→ Demander une démo

→ Contacter le service commercial

© 2025 Veeam Software. Tous droits réservés. Toutes les marques déposées sont la propriété de leurs détenteurs respectifs.

Découvrez la protection de Microsoft 365

Sauvegarder Microsoft 365 et Entra ID ensemble

Ce rapport explique :

- Les responsabilités qui incombent à votre entreprise concernant Microsoft 365
- Les raisons pour lesquelles il est indispensable de protéger les données Microsoft 365 aujourd'hui
- La marche à suivre pour identifier les brèches de sécurité dans votre entreprise
- Les avantages de l'utilisation d'un service de sauvegarde par rapport aux autres méthodes

→ 7 raisons cruciales de sauvegarder Microsoft 365

© 2025 Veeam Software. Tous droits réservés. Toutes les marques déposées sont la propriété de leurs détenteurs respectifs.