Renforcez Active Directory pour améliorer la sécurité et l'efficacité

AUTEURS :

Jay Bretzmann
Directeur de programme,
Produits de sécurité, IDC

Frank Dickson
Vice-président du programme,
Produits de cybersécurité, IDC

Active Directory et Azure Active Directory sont au cœur de nombreux programmes réussis de gestion des identités. Cependant, en raison du risque de violations, les entreprises doivent chercher à améliorer les capacités natives d'Active Directory avec des kits d'outils qui améliorent l'efficacité et la sécurité.

Ce qui est important

La sécurité des identités est une priorité pour les responsables de la gestion des identités et des accès (IAM), en particulier lorsqu'ils recherchent des solutions pour protéger leurs surfaces d'attaque. Avec 95 % des entreprises Fortune 1000 s'appuyant sur Microsoft Active Directory et Azure Active Directory (Azure AD) pour gérer et stocker les données d'identité et de compte, le besoin de renforcer la sécurité est essentiel.

En soi, Active Directory (y compris Azure AD) est un outil de gestion puissant, mais ses capacités natives peuvent être étendues et augmentées pour personnaliser l'expérience utilisateur à travers la sécurité, l'identité et ses rôles professionnels.

Ce document examine comment combler les lacunes dans la gestion et la sécurité d'Active Directory pour guider les entreprises qui doivent limiter la vulnérabilité et renforcer la sécurité informatique dans les environnements Active Directory.

Dans ce document

Cliquez ci-dessous pour accéder à chaque section.

Introduction 2

Avantages 4

Envisager One Identity pour la sécurité, l'automatisation et l'efficacité d'Active Directory . . 5

Conclusion 6

Active Directory est le fondement de la gestion des identités et des accès dans la plupart des entreprises et, en tant que tel, est probablement la technologie la plus cruciale sur le réseau.

Introduction

La sécurité et l'efficacité sont des priorités pour les dirigeants de l'IAM, d'autant plus qu'ils recherchent des solutions pour éviter les violations et sont confrontés à la mise en place de la sécurité basée sur une vérification systématique (dite « zero trust »). Active Directory est le fondement de l'IAM dans la plupart des entreprises et, en tant que tel, est probablement la technologie la plus cruciale sur le réseau. De plus en plus de systèmes et d'applications dépendent d'Active Directory et d'Azure AD pour l'authentification, la stratégie, les droits et la gestion de la configuration.

La sécurisation d'Active Directory/Azure AD est cruciale pour contrôler les risques et assurer la conformité. Cependant, maintenir Active Directory dans un état propre, organisé et sécurisé est un défi, en particulier pour les comptes d'utilisateurs, qui constituent la base de l'authentification et de l'accès aux réseaux, systèmes et applications. Les comptes d'utilisateurs sont difficiles à gérer sur plusieurs plateformes et tout au long de leur cycle de vie (de la création à la suppression) sans les outils appropriés. Pour ceux qui n'ont pas encore migré vers Azure AD, il est impératif qu'Active Directory soit aussi organisé que possible afin de ne pas aggraver les erreurs et perpétuer les problèmes de sécurité. La synchronisation de mauvaises données d'Active Directory vers Azure AD ne fait qu'empirer les choses. Par conséquent, l'utilisation d'une boîte à outils de gestion Active Directory comme solution pour aider à nettoyer l'annuaire avant la migration Azure AD est une étape importante.

Des gains en sécurité sont à portée de main pour Active Directory et Azure Active Directory

Alors que la sécurité « zero trust » est le cri de guerre du moment, l'autre cri de ralliement est la transformation numérique. Les entreprises cherchent à injecter de la technologie dans les processus métier pour améliorer la sécurité, offrir de l'empathie à grande échelle aux clients et augmenter l'agilité. Sans discipline, soin et planification délibérée, la transformation numérique peut générer pour les professionnels de la sécurité et de l'identité de grandes difficultés à gérer et à traiter, car chaque identité peut facilement devenir un flocon de neige (unique) basé sur les rôles.

Ainsi, les entreprises se demandent souvent comment faire de la sécurité « zero trust » une réalité dans leurs environnements. Alors que la pandémie de COVID-19 continue d'avoir un impact sur le monde et que les opérations commerciales s'adaptent, la transformation numérique a évolué vers la résilience des entreprises. Au fur et à mesure que les entreprises tentent de remédier à la pénurie de talents en matière de sécurité et aux demandes qui en résultent pour le personnel, nombre d'entre elles recherchent avec peine la plateforme de sécurité « zero trust » appropriée, résiliente et moderne.

Certes, des contrôles d'accès stricts aux points de terminaison, un accès simple et sécurisé et la suppression des conjectures lors des déploiements sont les principaux attributs de la sécurité « zero trust ». Ces derniers s'appuient sur un pilier de sécurité commun : l'identité. La base de ce pilier est Microsoft Active Directory. La question qui se pose aux professionnels de l'identité est de savoir comment libérer la puissance d'Active Directory pour conduire la transformation numérique et la sécurité « zero trust ».

Active Directory

Active Directory est au cœur de la plupart des stratégies d'identité d'entreprise. Active Directory est devenu fondamental pour la sécurité et l'informatique car il autorise tous les utilisateurs et ordinateurs dans un réseau de type domaine Windows, en attribuant et en appliquant des politiques basées sur des rôles ou des attributs définis d'une identité. À mesure que le monde passe de plus en plus au SaaS et cherche à mettre en œuvre des modèles de sécurité « zero trust » en raison des réalités du travail hybride, Active Directory est devenu encore plus important car Azure AD est la solution intégrée pour la gestion des identités dans Office 365.

Azure Active Directory

Avec l'ambition de constituer la base du travail hybride, Azure AD est la dernière offre de la famille. Azure AD est l'une des nombreuses technologies de sécurité développées pour prendre en charge Microsoft Azure (le service cloud). Comme les autres, il hérite immédiatement d'une opportunité d'étendre ce que les clients Azure peuvent accomplir en créant un marché de masse pour une approche d'identité et d'accès aux données basée sur des normes. Azure AD a fermé la boucle ouverte pour définir des implémentations commerciales compatibles SAML, OAuth, OData et SCIM disponibles dans des solutions gratuites et payantes (premium).

Les clients qui achètent des licences premium le font pour bénéficier d'un ou plusieurs des éléments suivants :

- Identification unique (SSO) illimitée
- Réinitialisation du mot de passe en libre-service (SSPR)
- Système de gestion des droits (EMS)
- Gestion des identités privilégiées (juste à temps [JIT])
- Accès conditionnel Azure AD
- Protection de l'identité Azure AD

Microsoft est sans doute en pole position pour atteindre la domination de l'identité dans le cloud et il le sait. Il s'agit d'une course qu'il ne peut perdre qu'en ne répondant pas aux exigences de connectivité et de communication informatiques des plateformes tierces. Il y a suffisamment d'ambiguïté dans les spécifications standard de l'industrie des applications Web nouvellement développées de nos jours pour qu'une mise en œuvre commerciale de facto soit une très bonne idée. Azure AD compte déjà plus de 1 000 implémentations SSO et 120 implémentations SCIM. C'est comme choisir DOS dans les premiers jours de l'informatique personnelle - saisissez suffisamment du marché initial et participez aux futures définitions des normes, et vous avez probablement une entreprise durable.

Azure AD gère actuellement plus de 425 millions d'utilisateurs actifs par mois (dont la majorité sont des abonnés Office 365) et traite plus de 90 milliards de demandes d'authentification quotidiennes. Sa base de clients premium comprend 300 000 entreprises et se développe rapidement. Il y a encore beaucoup de potentiel de hausse, et l'élan sans mot de passe se développera rapidement maintenant qu'Azure AD Conditional Access peut automatiquement implémenter des contrôles basés sur la réputation des utilisateurs, l'intégrité des appareils, les informations sur la source du réseau et les flux de renseignements sur les menaces.

Optimisation d'Active Directory pour un cas d'utilisation de sécurité avec de nouveaux outils

Active Directory et Azure AD sont des éléments de base de l'informatique ; cependant, les deux ont généralement servi dans un rôle d'accès informatique. Alors que les généralistes non informaticiens, à savoir les professionnels de la sécurité, cherchent à tirer parti de la puissance d'Active Directory pour générer des résultats en matière de sécurité et d'intégrité, ils constatent que les outils et interfaces existants ne sont pas conçus pour répondre à leurs besoins précis.

Les attributs essentiels pour un professionnel de la sécurité moderne sont les suivants :

- Délégation d'autorisations privilégiées
- Mûrissement de l'accès basé sur les rôles vers les attributs et les politiques
- Automatisation de la gestion du cycle de vie des identités
- Simplification des flux de travail et de l'allocation des accès sur plusieurs appareils à l'aide de certificats PKI et de la technologie push
- Facilitation des rapports pour la gouvernance et la conformité
- Intégration d'Active Directory avec des applications via des API pour partager le contexte d'identité
- Fourniture d'une automatisation (automatisation des processus robotiques [RPA]) pour réduire l'effort humain

Bien qu'Active Directory puisse être exploité pour la sécurité, il a été conçu pour servir plus que

les seuls professionnels de la sécurité ; c'est une plateforme polyvalente pourvue de nombreux maîtres. En conséquence, de nouveaux outils sont disponibles pour accroître l'envergure d'Active Directory et fournir une solution plus complète pour répondre aux besoins des professionnels de la sécurité et de l'identité dans la gestion d'Active Directory.

Avantages

Active Directory possède les composants nécessaires pour un déploiement réussi de la plateforme d'identité. À mesure que les entreprises se développent, le besoin de faire évoluer et d'améliorer la sécurité se fait plus pressant. L'objectif est de fournir des outils de gestion Active Directory augmentés qui permettent aux professionnels de la sécurité des identités de réaliser les capacités et de prévenir les violations en limitant les vulnérabilités, les menaces et les informations d'identification compromises, qui représentent collectivement 52 % des violations IaaS les plus récentes, selon l'étude IDC (voir la **figure 1**). Plus précisément, alors que le « manque d'outils de sécurité suffisants » a été cité comme la raison de 14 % des violations IaaS les plus récentes, il convient de noter que le traitement de chaque violation coûte des millions aux entreprises (le coût moyen d'une violation est de 3,92 millions de dollars, selon le rapport *2019 Cost of a Data Breach Report*, réalisé par le Ponemon Institute). La menace imminente et le poids de ce facteur conduisent au développement et à l'adoption de nouveaux outils de sécurité pour vous aider.

Pour maintenir et améliorer la sécurité, les entreprises ont besoin d'outils qui améliorent la précision, l'efficience et l'efficacité des professionnels de la sécurité. Ces outils devraient simplifier la gestion des environnements complexes, en fournissant des fonctionnalités telles que la délégation et la gestion faciles des autorisations et en garantissant la cohérence des données entre les déploiements Active Directory. L'automatisation est fondamentale, facilitant aisément les tâches de compte, la gestion dynamique des groupes, la création de flux de travail et la gestion du changement.

Avantages des kits d'outils de gestion Active Directory

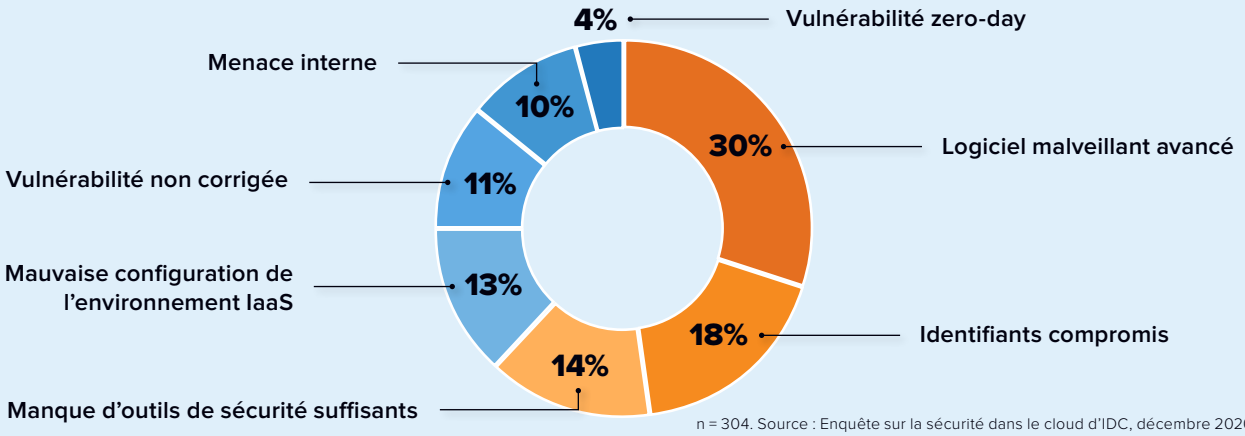
Les entreprises qui choisissent de se concentrer sur l'amélioration de leurs environnements Active Directory et Azure AD peuvent constater les avantages d'une efficacité et d'une sécurité améliorées grâce aux fonctionnalités suivantes :

- Simplifier la gestion des environnements complexes
- Activer la sécurité « zero trust » et la sécurité privilégiée pour Active Directory/Azure AD
- Automatiser les tâches de compte Active Directory/Azure AD et la gestion dynamique des groupes
- Déléguer et gérer les autorisations

FIGURE 1

Facteurs de violation

Q : Pour la violation la plus récente de vos environnements IaaS, quel a été le facteur prédominant qui a entraîné la violation ?



n = 304. Source : Enquête sur la sécurité dans le cloud d'IDC, décembre 2020

La possibilité d'attribuer des autorisations sans accorder des autorisations d'administrateur Active Directory complètes est essentielle. Sans une boîte à outils pour augmenter Active Directory, l'attribution de telles autorisations déléguées serait impossible.

- Créer des flux de travail et gérer le changement, en particulier pour les fusions et acquisitions, les déplacements/travail à domicile
- Assurer la cohérence des données et appliquer la politique

La possibilité d'attribuer à quelqu'un dans un service les autorisations pour configurer un nouvel utilisateur sans accorder les autorisations d'administrateur Active Directory complètes est essentielle. Sans une boîte à outils pour augmenter Active Directory, l'attribution de telles autorisations déléguées serait impossible.

Envisager One Identity pour la sécurité, l'automatisation et l'efficacité d'Active Directory

One Identity cherche à répondre aux besoins des professionnels de la sécurité et des identités dans la gestion d'Active Directory et d'Azure AD avec One Identity Active Roles. Des milliers d'entreprises dans le monde s'appuient sur Active Roles comme plateforme d'automatisation de compte utilisateur et de gestion de groupe. Ces entreprises utilisent Active Roles pour fournir des fonctionnalités de gestion des identités qui rendent les professionnels de la sécurité et des identités plus efficaces en tirant parti de l'automatisation pour permettre la délégation et un point d'administration unique.

Les principaux avantages sont les suivants :

- Administration simplifiée d'Active Directory/Azure AD
- Automatisation des tâches de compte Active Directory/Azure AD pour les nouveaux arrivants, les personnes qui changent de poste et celles qui quittent l'entreprise
- Réglementation de l'accès administrateur pour augmenter la sécurité des comptes privilégiés AD
- Prise en charge de plusieurs systèmes d'exploitation

Les capacités d'Active Roles qui répondent aux besoins exigeants des professionnels de la sécurité incluent :

- Gestion de tous les systèmes avec un seul point d'administration ou une interface centralisée
- Provisionnement accéléré avec des modèles d'accès simplifiés

De plus, Active Roles inclut les fonctionnalités suivantes :

- Moteur de flux de travail simplifié mais puissant
- Des « garde-fous » qui sécurisent la cohérence des données dans Active Directory
- Modifier l'historique du « qui/quoi/quand/où » d'objets particuliers

Défis

Comme pour beaucoup de choses dans la vie, on retire de toute plateforme d'identité ce que l'on y met. Active Directory ne fait pas exception. Active Roles peut fournir de puissants outils d'automatisation et de validation des données qui rendent les professionnels de la sécurité plus efficaces, mais les entreprises doivent toujours s'engager à tirer le meilleur parti de la plateforme. Active Directory peut être la plateforme de sécurité la plus puissante ou la plus grande vulnérabilité d'une entreprise ; c'est à elle de choisir. Avec la boîte à outils de gestion Active Directory appropriée pour augmenter Active Directory, une sécurité et une efficacité améliorées sont à portée de main.

Conclusion

Active Directory est une plateforme d'identité qui alimente les entreprises modernes. C'est une composante essentielle de la sécurité et de l'informatique. Active Directory authentifie et autorise tous les utilisateurs et ordinateurs d'un réseau de type domaine Windows, en attribuant et en appliquant des politiques basées sur des rôles ou des attributs définis d'une identité. Une grande partie de la transformation numérique trouve une connexion à Active Directory et à son cousin cloud, Azure AD.

Comme toute plateforme puissante, Active Directory sert de nombreux maîtres, notamment l'informatique, les opérations, la conformité et la sécurité, chacun avec ses propres buts et objectifs. Une plateforme à usage général, quelle que soit sa puissance, ne peut pas répondre de manière adéquate aux exigences ciblées d'un cas d'utilisation individuel. Depuis l'introduction d'Active Directory en 1999 et la prolifération ultérieure de la plateforme dans les entreprises, il est devenu nécessaire d'optimiser Active Directory pour le cas d'utilisation de la sécurité, rendant les professionnels de la sécurité à la fois plus efficaces avec l'automatisation et avec la validation des données. IDC pense que le marché des outils de gestion Active Directory sera de plus en plus important et que la transformation numérique continuera à générer des expériences immersives pour le travail hybride. Dans la mesure où One Identity peut répondre aux besoins décrits dans ce document avec Active Roles, l'entreprise a une opportunité significative de réussite.

Comme toute plateforme puissante, Active Directory sert de nombreux maîtres, notamment l'informatique, les opérations, la conformité et la sécurité, chacun avec ses propres buts et objectifs.

À PROPOS DES ANALYSTES

Jay Bretzmann
Directeur de programme,
Produits de sécurité, IDC

Jay Bretzmann est directeur de programme pour les produits de sécurité IDC, responsable de l'identité et de la confiance numérique et de la sécurité dans le cloud. Jay se concentre sur la gestion des identités, la gestion des accès privilégiés, la gouvernance des identités, la gestion des identités B2C et une multitude d'autres sujets liés à la sécurité des identités et du cloud.

En savoir plus sur Jay Bretzmann

Frank Dickson
Vice-président du programme,
Produits de cybersécurité, IDC

Frank dirige l'équipe qui produit des études convaincantes dans les domaines suivants : sécurité des réseaux ; sécurité des terminaux ; analytique, renseignement, réponse et orchestration de la cybersécurité (AIRO) ; Identité et confiance numérique ; juridique, risque et conformité ; sécurité des données; sécurité de l'IdO ; et sécurité du cloud. Sur le plan thématique, il fournit un leadership éclairé et des conseils aux clients sur une large gamme de produits de sécurité, notamment la sécurité des terminaux, la gestion des identités et des accès, l'authentification, l'analyse des menaces et les produits émergents conçus pour protéger les architectures et les modèles commerciaux en évolution.

En savoir plus sur Frank Dickson

MESSAGE DU SPONSOR

Avec des identités réparties dans divers ré-pertoires et plusieurs systèmes, et des auto-risations utilisateur assouplies, votre entreprise est vulnérable aux risques de cybersé-curité. One Identity Active Roles et Microsoft AD/Azure AD forment un binôme de choix pour améliorer la sécurité, assurer l'efficacité et atténuer les risques.

En savoir plus sur One Identity

En savoir plus sur Microsoft et Azure

IDC Custom Solutions

Cette publication a été produite par IDC Cus-tom Solutions. En tant que premier fournis-seur mondial d'informations sur le marché, de services de conseil et d'événements pour les marchés des technologies de l'information, des télécommunications et des technologies grand public, le groupe Custom Solutions d'IDC aide ses clients à planifier, commercia-liser, vendre et réussir sur le marché mondial. Nous créons des informations de marché ex-ploitables et des programmes de marketing de contenu influents qui produisent des ré-sultats mesurables.