Renforcer la sécurité grâce à une gestion intelligente des identités et des accès

Les solutions IBM Security permettent de protéger l'accès utilisateur, d'augmenter la conformité et d'atténuer les menaces internes

Points clés

- Permettre aux responsables d'entreprise de contrôler l'accès de leurs employés
- Améliorer l'assurance utilisateur à l'aide d'une authentification et d'analyses renforcés
- Renforcer les contrôles des identités et des accès (internes et externes) pour l'accès des utilisateurs de confiance situés au-delà des frontières de l'entreprise
- Améliorer la surveillance des activités utilisateur à travers les différents domaines de sécurité grâce aux renseignements de sécurité

Dans le monde multi-périmètres actuel, où les utilisateurs peuvent accéder à vos ressources d'entreprise à partir de n'importe quel terminal et où qu'ils se trouvent, la nécessité d'assurer la sécurité, la confidentialité et la conformité des interactions en ligne devient plus importante que jamais. L'utilisation croissante des technologies cloud et mobiles rend les limites de l'entreprise de plus en plus floues. Aujourd'hui, les entreprises ont besoin d'une approche centrée sur le facteur humain pour sécuriser les accès, et cela nécessite plus qu'une simple gestion des règles d'application des accès utilisateur et d'authentification unique. Les entreprises actuelles doivent être en mesure non seulement de contrôler l'accès à leurs ressources critiques, mais aussi de surveiller les actions des individus une fois qu'ils sont parvenus à y accéder. Elles peuvent ainsi identifier les comportements suspects et prendre les mesures appropriées pour réduire les risques et assurer une défense contre les menaces évoluées.

Les solutions de gestion des identités et des accès IBM® Security sont conçues pour prendre en charge une approche de la sécurité d'entreprise et de la conformité réglementaire centrée sur le facteur humain. La fourniture d'un accès basé sur les rôles aux personnes appropriées et au moment opportun, pour ensuite surveiller leur utilisation en vue de détecter les anomalies et les brèches de sécurité, permet aux entreprises de corriger les vulnérabilités de façon proactive et contribue à empêcher les activités malveillantes à venir.

Sécuriser l'entreprise étendue

Dans le monde entier, les entreprises permettent à un nombre croissant de types d'utilisateur, notamment les clients, les employés, les citoyens, les partenaires et les fournisseurs, d'accéder à des informations à travers le Web, le cloud et des environnements fédérés. Face au besoin de collaborer avec les partenaires commerciaux, d'interagir avec les fournisseurs tiers et les consommateurs en ligne et de prendre en charge les nouveaux services basés sur le cloud en toute sécurité, les fonctionnalités d'authentification et de contrôle des accès basées sur le risque jouent un rôle encore plus important. La migration vers le cloud, les réseaux sociaux et les environnements mobiles doit s'appuyer sur une infrastructure évolutive et sécurisée axée sur les identités, qui permette de surveiller et de protéger l'entreprise et ses données contre la menace, la fraude, et contre les attaques internes et externes.

Les solutions de gestion des identités et des accès d'IBM permettent aux entreprises d'adopter une approche intelligente et intégrée de la protection des identités au sein de l'entreprise étendue. Les solutions IBM incluent des fonctionnalités standard pour la mise en œuvre d'une authentification forte, de la gestion du cycle de vie et de l'accès par connexion unique, et les associent à des technologies de prochaine génération pour la reconnaissance des menaces, la gestion des règles, ainsi que la surveillance des utilisateurs et la génération de rapports sur les utilisateurs. De cette manière, les entreprises peuvent centraliser le contrôle des accès tout en bénéficiant également d'une visibilité sur « qui a accès à quoi » pour l'ensemble des ressources, tant sur le cloud que dans l'ensemble de l'infrastructure. En même temps, elles peuvent répondre aux exigences métier concernant la restriction des droits d'accès de l'utilisateur en fonction de son rôle, l'amélioration de la réactivité des clients et la réduction des coûts informatiques.

Fonctionnalités clés pour une sécurité intégrée

Les solutions de gestion des identités et des accès IBM Security peuvent vous aider à protéger vos ressources et vos informations d'entreprise contre les accès non autorisés, et cela sans affecter votre productivité.

Grâce à leur approche intégrée de la sécurité qui tire parti d'outils en libre-service et de la recertification automatisée, les solutions IBM peuvent rationaliser la mise en œuvre d'une gestion du cycle de vie de l'utilisateur conforme et basée sur des règles dans l'ensemble de l'entreprise, tout en veillant continuellement à l'application des règles de gouvernance et de conformité. En conséquence, les entreprises peuvent progresser vers une conformité durable, vers une réduction des coûts et des risques, et vers une amélioration des niveaux de service adaptées au monde multi-périmètres.

Prise en charge des initiatives de sécurité en cours

Les solutions de gestion des identités et des accès d'IBM peuvent à la fois répondre aux besoins tactiques immédiats de l'entreprise et jeter les bases stratégiques d'une réussite à long terme. Elles sont conçues pour donner aux responsables informatiques et commerciaux les moyens :

- De réagir efficacement au nombre croissant d'attaques axées sur les identités
- De protéger la collaboration et l'accès aux ressources en ligne dans les environnements mobiles, sociaux et cloud
- D'assurer la protection contre les menaces internes et contre les usurpations d'identité tout en veillant à la conformité
- D'adapter, simplifier et accélérer les services de sécurité pour les utilisateurs métier et le personnel informatique

Évaluer les besoins de sécurité par rapport aux priorités métier

En centralisant la gestion des profils utilisateur et des droits d'accès, les entreprises peuvent protéger leurs ressources critiques contre les menaces de sécurité, appliquer des règles de gouvernance et de sécurité, et maintenir la conformité aux réglementations les plus récentes. Lorsqu'ils sont alignés sur les priorités métier de l'entreprise, les projets de gestion des identités et des accès peuvent bénéficier d'une meilleure collaboration entre les cadres. Ils peuvent également tirer parti d'une évaluation attentive des problèmes de sécurité de l'entreprise, de ses règles et de ses pratiques en matière de contrôle d'accès, et de son environnement réglementaire. IBM recommande aux entreprises de tenir compte de ces facteurs lors de la détermination des priorités d'investissement et des exigences en matière de gestion des identités et des accès, puis de recourir à une évaluation formelle pour développer le plan détaillé de la mise en œuvre.

Les sections suivantes décrivent les façons dont l'offre IBM Security aide les entreprises à centraliser et à automatiser la gestion du cycle de vie des identités, le contrôle des accès et l'analyse de sécurité dans l'ensemble de l'entreprise, du grand système jusqu'au poste de travail.

Permettre aux responsables d'entreprise de contrôler les accès

IBM Security Identity Manager permet aux entreprises de mettre en œuvre des fonctions clés de gestion des identités, telles que l'application des accès utilisateur, le libre-service, la gestion des utilisateurs privilégiés et les renseignements de sécurité, pour assurer une visibilité des utilisateurs de bout en bout. Cette solution permet d'automatiser la gestion des rôles, des identités et des droits d'accès utilisateur tout au long du cycle de vie de l'utilisateur. IBM Security Identity Manager comprend des fonctions intégrées de gestion du cycle de vie des rôles qui peuvent favoriser la rationalisation du processus d'approbation de la structure des rôles et la réduction des erreurs lors de la validation des accès auprès de l'entreprise. Cette solution fournit un accès direct à des fonctions avancées de génération de rapports et d'analyse.

Appliquée aux plateformes existantes, au sein d'environnements répartis et grand système, IBM Security Identity Manager aide les administrateurs à centraliser la mise à disposition des définitions d'utilisateur et des services utilisateur de façon à minimiser les erreurs et les incohérences. Lorsqu'elle est intégrée à d'autres solutions IBM de gestion des identités et des accès, ainsi qu'au portefeuille IBM Security plus étendu, cette solution fournit une base solide pour la sécurisation des environnements dynamiques actuels.

IBM Security Identity Manager est fourni avec Identity Service Center, une interface utilisateur intuitive et conviviale qui peut aider les responsables d'entreprise à demander des droits d'accès pour leurs employés. Ces fonctions en libre-service peuvent aider les responsables d'entreprise à prendre des décisions d'accès intelligentes pour leurs employés tout en faisant gagner un temps précieux au personnel informatique.

Par ailleurs, les entreprises ont besoin de disposer d'un moyen de contrôler l'utilisation des données d'identification privilégiées et partagées pour se protéger contre les accès non autorisés. IBM Security Privileged Identity Manager peut contribuer à réduire le risque de menaces internes grâce à la centralisation de la gestion des identités partagées et privilégiées et à la génération de rapports sur les activités de ces utilisateurs. Les entreprises peuvent suivre et auditer les activités des utilisateurs privilégiés pour une gouvernance efficace, tout en réduisant le nombre total d'identités privilégiées nécessaires, ce qui permet d'améliorer le niveau général de sécurité et d'efficacité.

Renforcer les contrôles des identités et des accès (internes et externes)

IBM propose également des solutions de gestion des accès de premier plan qui aident les entreprises à bloquer les attaques externes, à protéger l'accès utilisateur dans les environnements cloud et mobiles, et à prévenir les violations de sécurité. Les solutions de gestion des accès IBM Security aident les entreprises à protéger leurs ressources informatiques critiques contre les accès non autorisés et à se conformer aux réglementations de sécurité. Grâce à un contrôle des accès pratique basé sur la connexion unique et sur le contexte, ces solutions permettent d'appliquer de façon proactive des règles d'accès établies afin d'empêcher les menaces et les usurpations d'identité à travers les canaux de collaboration mobile, sociale et sur le cloud. En outre, les solutions IBM permettent d'assurer le respect de la conformité en maintenant des pistes d'audit centralisées pour les demandes d'accès et en empêchant les accès non autorisés, tout en permettant aux administrateurs et aux utilisateurs d'être plus productifs.

Disponibles en tant qu'appliances physiques ou virtuelles, les solutions de gestion des accès IBM Security proposent un point unique d'autorisation pour les applications Web, cloud et d'entreprise, ce qui aide les entreprises à surmonter les difficultés liées à la mise en œuvre de règles de sécurité à travers un large éventail de ressources Web et de ressources d'application. Par exemple, IBM Security Access Manager for Mobile fournit des fonctionnalités axées sur les risques afin de protéger l'accès aux actifs informationnels de l'entreprise à partir de terminaux mobiles. Grâce à l'accès axé sur le risque, chaque transaction est évaluée à l'aide d'attributs statiques et contextuels pour calculer le risque. Cette évaluation du risque détermine si la demande d'un utilisateur pour accéder aux informations doit être autorisée, refusée ou autorisée moyennant une authentification supplémentaire. En conséquence, les entreprises peuvent fournir aux employés, aux partenaires, aux fournisseurs et aux clients un accès sécurisé aux informations et aux services dont ils ont besoin, et cela de façon systématique.

Améliorer l'assurance utilisateur à l'aide d'une authentification forte

Les solutions de gestion des accès IBM Security offrent également aux utilisateurs un accès par connexion unique rationalisé aux ressources protégées, même à partir de terminaux mobiles, ce qui contribue également à renforcer la sécurité de l'entreprise. Les utilisateurs doivent simplement mémoriser un identifiant et un mot de passe uniques. Non seulement l'expérience utilisateur s'en trouve simplifiée, mais cela permet également de réduire l'incidence des pertes de mots de passe, et donc de productivité pour les utilisateurs et le personnel informatique. En outre, les vulnérabilités de sécurité associées aux mots de passe consignés dans des emplacements non sécurisés sont minimisées. IBM Security Access Manager for Enterprise Single Sign-On prend également en charge une grande diversité de dispositifs d'authentification puissants, notamment les cartes à puce, les jetons, les badges et les dispositifs biométriques.

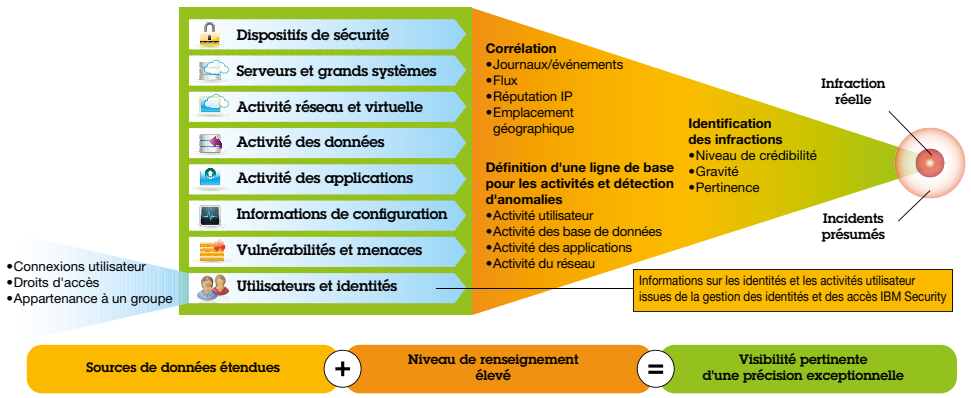
En centralisant l'authentification et l'autorisation des utilisateurs à l'aide des solutions IBM, les entreprises peuvent s'assurer que les utilisateurs sont effectivement ceux qu'ils prétendent être et appliquer des règles d'accès une fois que les utilisateurs ont été authentifiés. En outre, elles peuvent tirer parti de la gestion sécurisée des sessions en l'appliquant aux initiatives de portail et métier afin de protéger les transactions et les données sensibles.

Améliorer la surveillance des activités utilisateur à travers les différents domaines de sécurité

Le portefeuille intégré de solutions de gestion des identités et des accès IBM Security peut vous aider à centraliser la gestion du cycle de vie des utilisateurs au sein de l'entreprise, ce qui permet l'exécution systématique des règles de sécurité pour plusieurs applications et pour l'ensemble des catégories d'utilisateurs, y compris les utilisateurs privilégiés et mobiles. Le portefeuille fournit également des fonctions intégrées de génération de rapports d'audit et de détection en temps réel des fraudes internes basées sur IBM Cognos® qui tirent parti du renseignement de sécurité intégré.

IBM Security Identity and Access Assurance est une solution logicielle intégrée pour la protection des actifs métier et informatiques d'une entreprises contre les accès et les divulgations non autorisés. Cette solution IBM permet de renforcer la sécurité grâce à la gestion automatisée des identités et des accès dans différents environnements, y compris le cloud. Elle interagit avec un vaste ensemble de référentiels d'identités, gère facilement de gros volumes d'utilisateurs et permet l'automatisation des flux de travaux de processus, de telle sorte que les entreprises peuvent améliorer leur efficacité administrative et minimiser les erreurs coûteuses. La solution inclut les fonctionnalités intégrées de génération de rapports et de gestion des journaux d'IBM Security QRadar® Log Manager pour assurer la capture et le rassemblement automatique des activités d'accès utilisateur, afin de détecter les activités anormales ou non conformes et permettre le traitement et la correction des problèmes.

Étendre la gestion centralisée des identités grâce aux renseignements de sécurité



Les solutions de gestion des identités et des accès IBM Security s'intègrent avec IBM Security QRadar, elles fournissent les informations d'identité et d'activité utilisateur que QRadar met en corrélation avec d'autres données de sécurité en vue de détecter les comportements malveillants et y remédier.

Les solutions IBM Security QRadar permettent une surveillance contextuelle propice à l'action à travers l'ensemble de l'architecture informatique ; elles réduisent des milliers d'événements de sécurité à une liste gérable d'infractions présumées afin de faciliter la distinction entre les menaces réelles et les faux positifs. En intégrant QRadar aux solutions de gestion des identités et des accès IBM Security, les entreprises sont en mesure :

- De contrôler les privilèges utilisateur à travers une plateforme de gestion des règles de contrôle des accès centralisée
- D'identifier les menaces internes grâce à une visibilité accrue sur les utilisateurs, et pas seulement sur les terminaux, qui accèdent aux précieuses ressources en réseau
- D'améliorer la génération des rapports de conformité grâce au suivi de l'utilisation des droits d'accès utilisateur et des privilèges administratifs

Pourquoi IBM ?

La protection de l'accès utilisateur dans des environnements mobiles, cloud et en ligne, ou la gestion des groupes d'utilisateurs dynamiques dans des structures organisationnelles complexes, nécessite une approche intelligente plus intégrée de la gestion des identités et des accès. Des entreprises du monde entier font confiance aux solutions IBM Security pour mettre en œuvre une gestion de bout en bout des identités et des accès qui permet de renforcer la sécurité sans restreindre l'accès en temps voulu aux ressources critiques. Ces solutions assurent la visibilité et l'application des accès utilisateur aux données, aux applications et à l'infrastructure.

Pour en savoir plus

Pour en savoir plus sur les solutions IBM Security pour la gestion des identités et des accès, veuillez contracter votre représentant IBM ou votre partenaire commercial IBM, ou consulter le site Web suivant : **ibm.com**/security

À propos des solutions IBM Security

IBM Security offre l'un des portefeuilles de produits et services de sécurité d'entreprise les plus évolués et les plus intégrés. Ce portefeuille, qui s'appuie sur la recherche et développement IBM X-Force® de renommée mondiale, fournit des renseignements de sécurité qui aident les entreprises à assurer une protection holistique de leur personnel, de leurs infrastructures, de leurs données et de leurs applications, grâce à des solutions de gestion des identités et des accès, de sécurité des bases de données, de développement d'applications, de gestion du risque, de gestion des nœuds finaux, de sécurité du réseau, etc. Ces solutions donnent aux entreprises les moyens d'une gestion efficace du risque et d'une mise en œuvre intégrée de la sécurité pour les environnements mobiles, les médias sociaux et pour d'autres architectures métier d'entreprise. IBM dispose de l'une des plus importantes organisations de recherche et développement et de mise en œuvre dans le domaine de la sécurité. IBM gère 15 milliards d'événements de sécurité par jour dans plus de 130 pays, et possède plus de 3 000 brevets dans le domaine de la sécurité.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produit aux États-Unis d'Amérique
Avril 2014

Recyclable.

GMS10332-USEN-02