LIVRE BLANC

L'approche Zero Trust devient une réalité

Activer la sécurité unifiée des identités

Qu'est-ce que l'approche Zero Trust ?

Modèle éprouvé de mise en œuvre d'une sécurité robuste et sélective, l'approche Zero Trust consiste à supprimer les autorisations vulnérables, les accès inutiles et excessifs au profit d'une délégation spécifique et d'un provisioning approprié avec une granularité fine.

- L'activation de l'approche Zero Trust élimine le partage des mots de passe d'administrateur et permet une authentification individuelle et dynamique pour chaque action administrative.
- Le modèle d'accès de moindres privilèges consiste à délivrer uniquement les autorisations dont un administrateur a besoin pour faire son travail, ni plus ni moins.

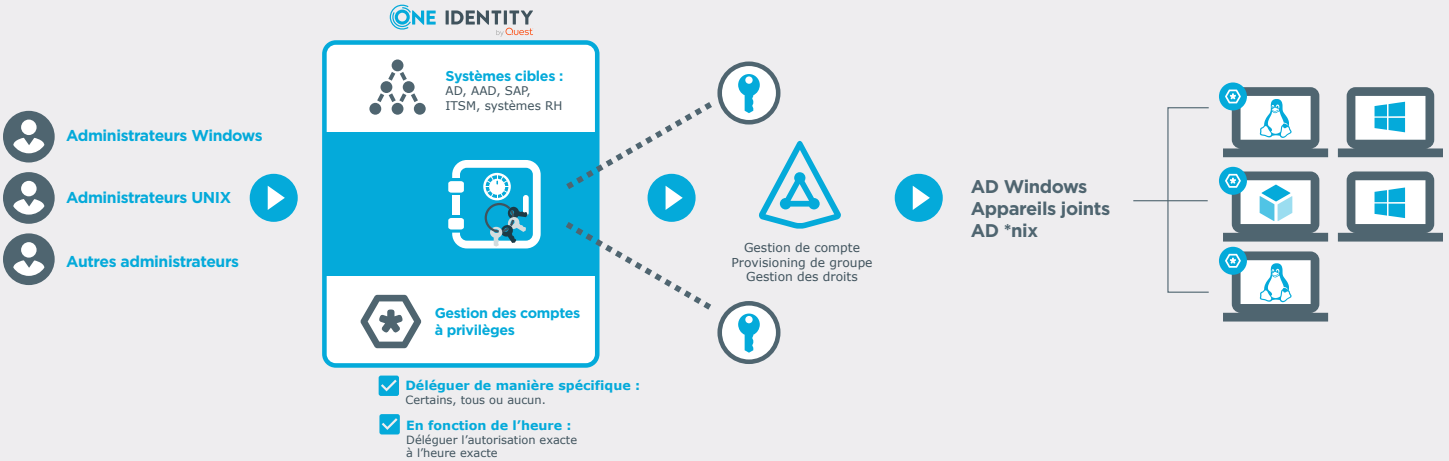
Présentation

Le concept Zero Trust est en train de devenir rapidement le modèle de sécurité de prédilection des responsables informatiques, car il s'agit d'une approche valide et fiable de la sécurité des identités. Avec une méthode plus intentionnelle pour la sécurité et la gestion des accès à privilèges, son mantra « ne jamais faire confiance, toujours vérifier » diffère du modèle d'accès de moindres privilèges. Ce résumé technique couvre les éléments nécessaires à la mise en place d'une politique de sécurité solide, notamment les points suivants :

- L'établissement de « l'identité comme périmètre » répond à de nombreux principes fondamentaux de ce modèle de sécurité. Cette approche nécessite notamment une solution unifiée pour un provisioning fiable, la gestion des droits, la gestion des accès à privilèges, une authentification forte, l'accès sécurisé et la gouvernance.
- Dans un modèle Zero Trust, toutes les communications sont sécurisées, mais sans confiance.
- La mise à disposition d'une « source unique de vérité » (des données d'identité centralisées et synchronisées) permet aux organisations de contrôler totalement les identités et les ressources. Cela n'est réellement possible qu'une fois ce concept de droit établi.
- Aucune pièce du puzzle n'offre à elle seule un modèle de sécurité complet, mais une bonne association de solutions, oui.

Pour de nombreuses organisations, l'approche Zero Trust est accessible lorsqu'elles s'appuient sur des solutions modulaires et intégrées, notamment la gestion des accès à privilèges, la gestion d'Active Directory (AD)/Azure AD, la collecte d'événements et

L'approche Zero Trust avec One Identity



la gouvernance et l'administration des identités. Cette approche intégrée vous permet de respecter les principes fondamentaux de la sécurité Zero Trust tout en offrant une expérience optimale à l'utilisateur final.

Passer au modèle de sécurité Zero Trust

À mesure que les efforts de modernisation transforment les modes fondamentaux d'application, de consommation et d'accès aux technologies informatiques, la sécurité des identités devient de plus en plus importante. Des initiatives telles que la modernisation des applications, la priorité donnée au Cloud, les innovations en matière de réseaux, comme les réseaux software-defined (SDN) et les pressions concurrentielles, rendent difficiles la gestion et la protection de l'accès des utilisateurs et des autres ressources non humaines. Comment une organisation peut-elle mettre en œuvre en toute sécurité des technologies basées sur le Cloud tout en conservant les ressources critiques sur site ?

Même si nous aimerions tous avoir des processus clairs et nets, la réalité est que la plupart des organisations vont exploiter un mélange hybride de systèmes locaux et Cloud dans un avenir prévisible. Maintenir la sécurité, répondre aux exigences de conformité et offrir une expérience utilisateur fluide peut paraître une tâche impossible.

Elle ne devrait pas l'être. Vous pouvez y parvenir en introduisant ce modèle de sécurité au fur et à mesure de votre transformation numérique. Une fois ce modèle en place, vous pouvez réduire la complexité et définir des mesures de référence afin de créer des bonnes pratiques personnalisées pour la sécurité des systèmes d'informations et des identités.

Architecture Zero Trust du NIST:

1. Toutes les sources **de données et les services informatiques** sont considérés comme des ressources.

2. Toutes les **communications sont sécurisées**, où que se trouve réseau.

3. L'accès aux ressources individuelles de l'entreprise est accordé pour **le temps de la session**.

6. Toutes les authentifications et autorisations des ressources sont dynamiques et strictement **appliquées avant que l'accès ne soit autorisé**.

4. L'accès aux ressources est déterminé par une **stratégie dynamique**, notamment l'état observable de l'identité du client, de l'application/du service et de l'actif demandeur, et peut inclure d'autres attributs comportementaux et environnementaux.

5. L'entreprise **surveille et mesure** l'intégrité et le niveau de sécurité de tous les actifs possédés et associés.

7. L'entreprise recueille autant d'informations que possible sur **l'état actuel des actifs, de l'infrastructure réseau et des communications** et les utilise pour améliorer sa politique de sécurité.

Référence : NIST SP 800-207 « Zero Trust Architecture »

L'identité forme le nouveau périmètre

De plus en plus de fonctions de mise en réseau faisant partie d'un environnement de réseau virtuel, les pare-feu et le routage statique traditionnels sur site ont été remplacés par des ressources virtuellement couplées. La sécurité de l'identité forme le nouveau périmètre. La protection des identités nécessite une authentification forte, un accès sécurisé et une gouvernance. Dans un modèle de sécurité Zero Trust, toutes les communications sont sécurisées, mais sans confiance.

Une solide base de sécurité des identités qui s'adapte dynamiquement et fournit des stratégies unifiées et un contrôle d'accès pour les ressources locales ou dans le Cloud est un élément essentiel de ce nouveau modèle. La mise à disposition d'une « source unique de vérité » (données d'identité centralisées et synchronisées) pour garantir les droits, les attributs et les prérogatives tout au long du cycle de vie de l'identité donne aux organisations un contrôle total. Le modèle Zero Trust n'est réellement possible qu'une fois ce concept de droit établi.

Les sept principes fondamentaux

Le projet NIST SP800-207 définit les principes de base du modèle Zero Trust. Ces principes aident les fournisseurs à concevoir des solutions afin que les utilisateurs de technologies puissent adopter des services qui leur permettent de mettre en œuvre le modèle de sécurité de manière efficace et prévisible.

Ces principes prévoient notamment que :

1. **Toutes les sources de données et les services informatiques sont considérés comme des ressources.**
2. **Toutes les communications sont sécurisées, où que se trouve réseau.**
3. **L'accès aux ressources individuelles de l'entreprise est accordé pour le temps de la session.**

   Ce concept clé de la sécurité des identités se concentre spécifiquement sur la gestion des privilèges élevés. Si une personne ou un compte a besoin de privilèges élevés pour effectuer une tâche spécifique, elle n'a probablement pas besoin de cette autorisation en permanence. C'est ce que One Identity Manager, Active Roles et One Identity Safeguard (avec le provisining juste-à-temps) permettent de faire.
4. **L'accès aux ressources est déterminé par une stratégie dynamique, notamment l'état observable de l'identité du client, de l'application/du service et de l'actif demandeur, et peut inclure d'autres attributs comportementaux et environnementaux.**

   Le mot clé ici est « dynamique ». Une stratégie dynamique permet de modifier la fonctionnalité de l'accès pour répondre aux besoins spécifiques de l'utilisateur en temps réel. Les solutions Identity Manager et Active Roles offrent toutes deux cette fonctionnalité ainsi qu'une piste d'audit élaborée pour prouver où l'accès a été accordé (ou refusé), qui l'a demandé, quand il a été accordé et quand il a été supprimé.

5. **L'entreprise surveille et mesure l'intégrité et le niveau de sécurité de tous les actifs possédés et associés.**

   Les « actifs » de l'entreprise englobent de nombreux éléments. La visibilité des personnes ayant accès, de la manière dont elles ont été autorisées et même des vulnérabilités de sécurité calculées sur la base d'un modèle de privilèges fournit des informations essentielles à l'entreprise pour la prise de décision. One Identity Manager se concentre sur l'identité à la fois comme un actif et comme un sujet à gérer afin que des informations précises soient utilisées pour prendre des décisions d'accès et fournir des rapports.

6. **Toutes les authentifications et autorisations des ressources sont dynamiques et strictement appliquées avant que l'accès ne soit autorisé.**

   La stricte application du contrôle d'accès est une nécessité absolue pour tout système. Les solutions One Identity permettent de rendre le contrôle d'accès dynamique pour répondre à tout besoin réglementaire ou métier en détectant les changements d'identité et en manipulant instantanément les systèmes finaux pour refléter le changement d'accès requis.

7. **L'entreprise recueille autant d'informations que possible sur l'état actuel des actifs, de l'infrastructure réseau et des communications et les utilise pour améliorer sa politique de sécurité.**

   La visibilité est essentielle pour garantir la sécurité de tout système. Qu'il s'agisse de l'état actuel de l'accès ou des événements générés par le changement, les solutions One Identity couvrent ce principe de base. Alors que One Identity Manager fournit une visibilité et une gouvernance des états et des changements d'accès, Active Roles audite les changements apportés aux objets Active Directory et Safeguard contrôle les accès à privilèges, One Identity syslog-ng collecte toutes les données d'événements pour garantir une connaissance complète de la situation de l'entreprise.

Aucune solution ne fournit un « bouton magique » pour mettre en œuvre un modèle Zero Trust. Cela doit devenir un état d'esprit lors de la mise en œuvre de nouveaux systèmes, applications, réseaux et même de la sécurité physique. L'adoption et l'association de ces concepts fournissent un cadre permettant de garantir que les entreprises utilisent toutes les possibilités pour sécuriser leur infrastructure. La sécurité des identités joue un rôle important dans la main-d'œuvre moderne.

Bien qu'aucune pièce du puzzle ne permette à elle seule d'atteindre le niveau de confiance zéro, une association efficace des pièces le permettra. L'exploitation de la plateforme de sécurité unifiée des identités de One Identity, notamment nos offres de gestion des accès à privilèges, de gestion d'Active Directory (AD)/Azure AD, de collecte d'événements et de gouvernance et d'administration des identités, permet de mettre en œuvre le modèle de sécurité tout en offrant une expérience satisfaisante à l'utilisateur final.

Comment faire pour que l'approche Zero Trust devienne une réalité ?

Pour que les organisations puissent y parvenir, une approche intégrée avec une plateforme de sécurité unifiée des identités est nécessaire. Si l'élaboration de stratégies adaptées et efficaces pour sécuriser et gérer les identités peut s'avérer très complexe, la mise en œuvre de ces stratégies reste l'élément clé du point de vue de la sécurité.

Les solutions One Identity permettent aux entreprises disposant de divers environnements de mettre en œuvre des pratiques centrées sur l'identité qui suivent l'architecture Zero Trust du NIST. Le NIST nous fournit des directives technologiques solides pour nous aider à progresser de manière significative vers la sécurisation des informations critiques. Si ces concepts ne ciblent pas spécifiquement les environnements locaux ou Cloud, il apparaît essentiel de les appliquer aux systèmes qui fournissent chaque jour des décisions d'accès dans chaque entreprise.

One Identity fournit les solutions qui répondent parfaitement aux principes spécifiques du NIST. Nos solutions permettent de :

Contrôler l'accès avec One Identity Manager, qui est spécialement conçu pour contrôler l'accès, garantir la mise en œuvre du modèle de moindres privilèges et supprimer dynamiquement l'accès lorsqu'il n'est plus nécessaire pour tout système connecté.

Appliquer l'accès de moindres privilèges avec Active Roles, qui permet d'appliquer les concepts Zero Trust à Active Directory en fournissant une gestion du cycle de vie des comptes, des rôles et un contrôle d'accès dynamiques, et en appliquant strictement le modèle de moindres privilèges pour l'accès à Active Directory et à tous les systèmes attachés.

Gérer les accès à privilèges avec Safeguard, qui offre une gamme complète de solutions de gestion des accès à privilèges pour garantir que les identités et les comptes puissants qui font fonctionner l'entreprise sont sous contrôle strict, ce qui peut être prouvé par des pistes d'audit et des rapports détaillés.

Recueillir les logs avec syslog-ng pour une gestion flexible et évolutive des logs dans toute l'entreprise afin de garantir l'utilisation la plus efficace et la plus rentable de SEIM.

À propos de One Identity

One Identity, une entité Quest, aide les organisations à mettre en place une stratégie de sécurité axée sur les identités, aussi bien sur site, dans le Cloud ou dans un environnement hybride. Avec notre vaste portefeuille intégré d'offres de gestion des identités, comprenant la gestion des comptes, l'administration et la gouvernance des identités, ainsi que la gestion des accès à privilèges, les organisations peuvent réaliser tout leur potentiel et bénéficier d'une sécurité efficace grâce à une stratégie axée sur les identités, qui assure un accès adéquat à tous les types d'utilisateurs, tous les systèmes et toutes les données. En savoir plus sur le site OneIdentity.com

WhitepaperAD-MakingZeroTrustReal-RS-FR-WL-65397