ORACLE

Zero trust pour une résilience maximale

Un guide pratique de l'approche de sécurité moderne « ne jamais faire confiance, toujours vérifier »

Table des matières

Il est temps d'adopter l'approche zero trust

Lorna Garey
Senior Writer

Vous cherchez une approche plus proactive de la sécurité ? Le Pentagone adopte plus rapidement que prévu son architecture de zero trust. En effet, l'échéance, initialement fixée à 2027, a été avancée de 12 mois. Un observateur a interrogé environ 650 professionnels de l'informatique et de la cybersécurité dans divers secteurs et a constaté qu'un peu plus d'un tiers ont déjà mis en œuvre une stratégie de zero trust et que 47 % supplémentaires prévoient de le faire dans moins d'un an.

Ce n'est pas votre cas ? Alors, il est peut-être temps d'explorer les moteurs de ce changement stratégique majeur.

La sécurité zero trust, également appelée sécurité sans périmètre, utilise l'authentification et l'autorisation fréquentes, le chiffrement et la segmentation fine pour protéger les ressources. Aucune entité (personne, appareil ou application, à l'intérieur ou à l'extérieur du réseau) n'est approuvée par défaut. Les entreprises partent du principe que leurs systèmes sont déjà compromis. Dès lors, elles surveillent et réauthentifient en permanence les utilisateurs, les services et les appareils. Elles accordent l'accès en fonction des données (le contexte de la demande, le niveau de confiance et la sensibilité de la ressource) et avec uniquement les autorisations nécessaires pour accomplir la tâche. La segmentation limite les accès d'une entité sans réauthentification, empêchant les pirates de naviguer librement dans le réseau et réduisant le temps de réponse à une violation.

Ce changement peut sembler spectaculaire par rapport au modèle traditionnel « châteaux et fossés » et c'est bel et bien le cas. Bien qu'une approche progressive soit courante, le passage à la zero trust nécessite beaucoup de travail, de ressources et de sensibilisation. Toutefois, il est sans doute nécessaire de se prémunir des menaces auxquelles la plupart des organisations seront confrontées en 2025 et dans les années à venir. Nous comparons les contrôles de sécurité aux freins d'une voiture : ils sont là pour vous permettre d'aller vite tout en sachant que vous pourrez les utiliser au besoin. Sans les mesures de sécurité qu'ils jugent nécessaires pour protéger l'entreprise, les responsables informatiques peuvent adopter une attitude attentiste quand ils doivent valider les nouvelles technologies et utiliser des données sensibles.

À qui profite l'approche zero trust ?

Une approche zero trust positionne les contrôles de sécurité stratégiquement sur l'ensemble du réseau, pas seulement au périmètre. Cela rend une architecture de zero trust particulièrement efficace pour les entreprises qui exécutent des workloads dans le cloud, partagent des données avec des partenaires de confiance et prennent en charge les collaborateurs et les emplacements distants et une diversité d'appareils. Pourtant, la zero trust ne se cantonne pas aux workloads cloud. Le succès réside dans la standardisation de ces principes dans les environnements on-premises, hybrides et cloud.

Le Pentagone est un exemple d'un écosystème extrêmement complexe avec une approche zero trust. David McKeown, Deputy Chief Information Officer for Cybersecurity du ministère de la Défense des États-Unis, a déclaré devant des journalistes que son équipe adopte une approche d'implémentation hybride qui comprend l'intégration de nouveaux outils et fonctionnalités, l'adoption de solutions de cloud commercial qui ont des capacités de zero trust intégrées ainsi que l'utilisation de clouds privés on-premises spécialement conçus.

Comme le démontre le ministère de la Défense, la sécurité zero trust n'est pas un produit ou un service qui peut être activé en appuyant simplement sur un bouton, bien que la bonne technologie soit essentielle. C'est plutôt une façon de travailler qui peut exiger des ajustements dans la culture, la philosophie et les flux de travail.

Comment fonctionne une approche de sécurité zero trust ?

Par défaut, aucune entité n'est digne de confiance et reçoit l'accès avec le moins de privilèges possible. Le réseau est segmenté pour empêcher toute intrusion d'un acteur malveillant.

*****

Authentification :
Qui êtes-vous ? Utilisez des mots de passe robustes et une identification multifacteur.

Le contexte :
Où êtes-vous et dans quelle mesure votre appareil est-il sécurisé ? Limitez l'accès en fonction des données contextuelles.

Le moindre privilège :
Quel est l'accès minimum requis pour répondre à votre demande ? Bénéficiez d'autorisations d'accès limitées dans le temps et dans les ressources.

La microsegmentation du réseau dans la mesure du possible est une pierre angulaire de l'approche zero trust.

Comment vendre les avantages de la zero trust ?

Les dirigeants d'entreprise peuvent vous demander pourquoi il faut adopter maintenant l'approche zero trust. Les raisons sont multiples. Les entreprises ont plus d'options pour l'authentification, grâce à des logiciels, des services et du matériel qui prennent de plus en plus en charge la biométrie et les méthodes de connexion plus évoluées que les mots de passe.

En outre, l'IA générative peut aider à mettre en place une architecture zero trust de plusieurs manières :

- Les systèmes automatisés de détection des menaces alimentés par l'IA générative peuvent analyser d'importants volumes de trafic réseau et de journaux système pour identifier les anomalies et les menaces et, lorsque cela est autorisé, les arrêter en temps réel.
- L'IA peut définir le comportement normal des utilisateurs et analyser des modèles pour détecter une activité anormale qui pourrait indiquer, par exemple, qu'un acteur malveillant essaie de se connecter avec des informations d'identification volées ou de télécharger des données précieuses.
- Les agents d'IA peuvent automatiser le provisionnement et le déprovisionnement, réduisant ainsi le risque d'erreur humaine.

De plus, les agents d'IA peuvent vérifier que chaque système ou utilisateur dispose du privilège d'accès minimum nécessaire pour effectuer le travail, un autre principe de la zero trust. Ces facteurs se combinent pour faire de 2025 l'année où le modèle zero trust devient plus tangible pour une majorité d'organisations.

Concept clé : SSO sur les périphériques sécurisés

L'authentification unique (SSO) sur les périphériques sécurisés permet aux utilisateurs d'accéder à plusieurs applications et services avec une authentification unique, à condition qu'ils utilisent un appareil sécurisé. Cette approche peut simplifier le processus de connexion et améliorer la sécurité en réduisant le nombre de mots de passe ou d'autres formes d'authentification que les utilisateurs doivent utiliser.

Pour commencer, enregistrez les périphériques sécurisés. Cela implique souvent de vérifier les spécifications et la sécurité d'un périphérique. Une fois qu'un appareil est sécurisé, son utilisateur peut être en mesure de se connecter avec moins de facteurs d'authentification supplémentaires. Cependant, le service informatique doit surveiller en permanence les périphériques de confiance pour détecter les changements dans leurs postures de sécurité. Le statut de confiance peut être révoqué ou, si un périphérique est jugé risqué, notamment en raison de son emplacement ou de logiciels obsolètes, une authentification ou des actions supplémentaires pour se mettre en conformité peuvent être requises.

Concept clé : gouvernance automatisée des identités

La gouvernance des identités est le processus de gestion des identités numériques et des droits d'accès au sein d'une entreprise. Elle implique l'automatisation de la gestion du cycle de vie des identités, l'application de stratégies d'accès et la séparation des tâches avec des contrôles d'accès stricts, et la surveillance des activités des utilisateurs conformément à l'approche zero trust consistant à n'accorder que le privilège minimal nécessaire.

La gestion du cycle de vie des identités nécessite la possibilité de créer, modifier et supprimer automatiquement des comptes, d'affecter des rôles aux utilisateurs en fonction de leurs fonctions et responsabilités professionnelles en fonction des stratégies de séparation des tâches et de définir des contrôles d'accès granulaires basés sur des attributs pertinents.

L'application de stratégies d'accès pour les comptes utilisateur et les données sensibles consiste à accorder uniquement les privilèges minimaux pour effectuer des tâches, puis à surveiller et à vérifier régulièrement les autorisations et les activités afin de détecter les anomalies et les menaces potentielles et de vérifier la conformité aux réglementations du secteur et aux politiques internes.

Concept clé : MFA résistant à l'hameçonnage et sans mot de passe

Les méthodes d'authentification multifacteur (MFA) résistantes à l'hameçonnage visent à empêcher les pirates d'intercepter les codes de mot de passe à usage unique (OTP), tandis que l'accès sans mot de passe est une approche de sécurité qui supplante ou complète les mots de passe avec des méthodes d'authentification plus strictes. Les utilisateurs peuvent s'authentifier en utilisant des facteurs biométriques, tels qu'une empreinte digitale ou la reconnaissance faciale, en plus d'un appareil de confiance, tel qu'un smartphone. Les entreprises peuvent également émettre des clés de sécurité physiques qui fournissent une authentification forte sans mot de passe. De plus, le service informatique peut évaluer le risque de chaque tentative d'authentification, par exemple d'un utilisateur qui voyage ou qui n'a pas régulièrement utilisé le système, et exiger des étapes de vérification supplémentaires si nécessaire.

En plus de réduire le risque de violation de mot de passe, les entreprises pourraient économiser de l'argent en réduisant le nombre de réinitialisations de mot de passe et le verrouillage de compte. L'IA peut également jouer un rôle en validant régulièrement l'identité d'un utilisateur via des scans faciaux passifs ou éventuellement une reconnaissance vocale, ce qui améliore encore la sécurité.

Une approche modélisée

Les entreprises n'ont pas besoin de réinventer la roue. Plusieurs agences ont publié gratuitement des architectures de modèles de zero trust et des conseils techniques.

Cybersecurity and Infrastructure Security Agency Zero Trust Maturity Model
CISA est une agence américaine responsable de la protection des infrastructures critiques et de la promotion de la cybersécurité. La version 2.0 de son modèle Zero Trust Maturity Model (ZTMM) comprend cinq piliers plus plusieurs principes généraux et vise à être adaptable pour un environnement commercial, de sécurité et technologique en évolution rapide.
CISA

Defense Information Systems Agency Zero Trust Reference Architecture
Ce document intègre les principes de sécurité zero trust dans toute l'architecture et est utilisé par le ministère de la Défense et d'autres agences gouvernementales des États-Unis.
DISA

National Cyber Security Centre Zero Trust Architecture Design Principles
Ce cadre flexible décrit huit principes pour aider à mettre en œuvre une architecture de réseau zero trust. Le NCSC est une entité du gouvernement britannique qui fournit des conseils et des conseils aux entreprises, aux autres agences et aux particuliers.
NCSC

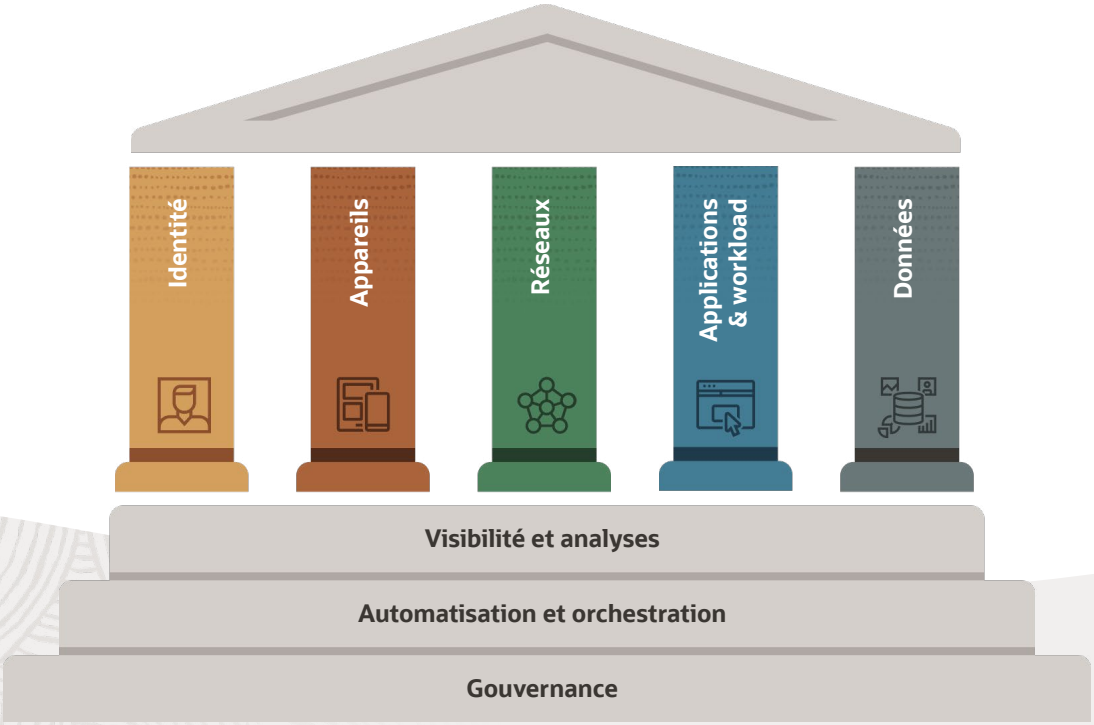
National Institute of Standards and Technology Zero Trust Architecture
Ce cadre, publication spéciale 800-207, fournit une approche complète de l'implémentation zero trust couvrant les identités, les appareils, les réseaux et les applications. NIST, une agence non réglementaire au sein du ministère du Commerce des États-Unis, promeut l'innovation et la compétitivité industrielle.
NIST

5 piliers du succès

Beaucoup de ces modèles de zero trust sont basés sur des piliers et des principes. L'US CISA ZTMM, par exemple, repose sur deux principes fondamentaux :

- L'objectif est d'éloigner les parties non autorisées des données et des services en rendant l'application du contrôle d'accès aussi précis que possible.
- Aucun utilisateur ou actif ne doit faire l'objet d'une confiance implicite. En effet, on part du principe qu'une violation a déjà eu lieu ou se produira et, par conséquent, aucune entité ne doit avoir accès à des informations sensibles sur la base d'une vérification unique effectuée au périmètre. Au lieu de cela, chaque utilisateur, dispositif, application ou service doit être connu et continuellement vérifié avec chaque transaction et l'intégrité et le comportement de l'appareil de l'utilisateur continuellement évalué et surveillé.

Le ZTMM classe également la maturité le long de chaque pilier, d'une approche traditionnelle à une approche optimale, afin que les équipes puissent évaluer comment elles se comportent dans chaque domaine. Examinons brièvement les piliers du ZTMM et ce que chacun prescrit.



Pilier : Identité

La sécurité zero trust repose sur une gestion forte des identités et des accès (IAM), soutenue par un service d'administration et de gouvernance des identités qui offre une visibilité sur les systèmes cloud et on-premises. L'identité peut être associée à un humain, une application ou un appareil et est gérée avec une plateforme d'IAM qui confirme qu'un utilisateur est celui qu'il dit être et utilise un appareil connu. Bien qu'une plateforme d'IAM capable puisse servir de référentiel d'identités principal, de nombreuses entreprises disposent de plusieurs systèmes de gestion des identités, qui doivent tous être gérés pour atteindre une architecture zero trust.

> L'IA peut vous aider en générant des révisions d'accès basées sur les analyses qui fournissent des informations sur les autorisations d'accès et les stratégies d'infrastructure cloud et signalent les anomalies potentielles.

Parmi les autres catalyseurs de ce pilier figurent le contrôle d'accès reposant sur des rôles (RBAC), le contrôle d'accès reposant sur des attributs (ABAC) et des technologies de contrôle d'accès reposant sur des politiques (PBAC). Un système RBAC affecte des autorisations aux utilisateurs en fonction de leurs rôles au sein d'une organisation et d'une application. Il peut également dicter les données auxquelles un utilisateur d'un rôle donné peut accéder et la façon dont il peut agir dessus.

L'ABAC est une approche plus granulaire qui prend en compte des attributs supplémentaires des ressources et des utilisateurs, tels que l'heure de la journée, l'emplacement et la sensibilité des données. Le PBAC est un système encore plus avancé et flexible qui permet aux organisations de définir des stratégies complexes basées sur des règles qui spécifient qui peut accéder à quelles ressources dans quelles conditions. Les points d'application des politiques (PEP) aident à réglementer l'accès en évaluant les demandes par rapport à ces règles. Par exemple, par stratégie, un professionnel RH peut ne voir que certaines données dans un CRM, telles que les statistiques de performance des ventes.

Bien que la norme XACML (Extensible Access Control Markup Language) définisse des stratégies de sécurité, les entreprises doivent vérifier que la plateforme de contrôle d'accès qu'elles sélectionnent peut fonctionner avec leurs applications critiques. Open Policy Agent, un moteur de stratégie flexible et open source qui unifie l'application des stratégies sur les différentes couches de l'infrastructure d'une organisation, devient une option populaire en tant qu'extension de XACML.

L'authentification forte est un autre élément important de ce pilier. Quelqu'un peut commencer par un nom d'utilisateur et un mot de passe, ce qu'il sait, qui est le premier facteur, puis être invité à fournir un deuxième facteur, peut-être un code d'un appareil enregistré ou une empreinte digitale.

Le provisionnement de l'accès juste à temps (JIT) accorde le niveau d'accès minimum requis pour effectuer une tâche spécifique et uniquement pour la durée nécessaire. L'accès est provisionné à la demande et automatiquement révoqué lorsqu'il n'est plus nécessaire.

Pilier : Appareils

Les appareils ne sont pas seulement des smartphones et des PC, mais aussi des systèmes utilisés au cœur d'un data center privé ou cloud. Une gestion efficace des périphériques dans le cadre d'une approche une zero trust nécessite un inventaire dynamique des ressources, y compris du matériel, des logiciels, des microprogrammes et des configurations, selon notre exemple de modèle CISA. En général, il est recommandé d'accorder des autorisations de manière prudente et de limiter la durée pendant laquelle un périphérique peut rester connecté au serveur en fonction de l'inactivité ou d'une durée de session définie.

L'activation des technologies pour ce pilier commence par les systèmes de sécurité des terminaux et de gestion des appareils mobiles (MDM) car le principe « ne jamais faire confiance, toujours vérifier » signifie que chaque demande d'accès doit être complètement authentifiée et explicitement autorisée. Les solutions de sécurité des périphériques surveillent les appareils, y compris les ordinateurs de bureau, les ordinateurs portables et les serveurs, pour vérifier qu'ils sont conformes aux politiques de sécurité, tandis que la MDM aide le service informatique à gérer les appareils mobiles. Ensemble, ils contribuent à créer un cadre de sécurité robuste qui prévoit l'accès aux informations d'identité et contextuelles.

Les systèmes de détection et de réponse (EDR) des terminaux détectent les menaces sur les appareils, y compris les ordinateurs portables, les ordinateurs de bureau et les serveurs, et y répondent. L'EDR repose sur des analyses avancées et le machine learning pour collecter et analyser en permanence des données qui peuvent, par exemple, identifier une utilisation abusive potentielle d'un appareil ou d'une infection par un logiciel malveillant.

Pilier : Réseaux

L'approche zero trust prend ses distances avec la sécurité traditionnelle axée sur le périmètre. Dans l'exemple CISA, les équipes informatiques doivent gérer précisément les flux de trafic internes, isoler les hôtes, appliquer le chiffrement, segmenter l'activité, positionner les contrôles de sécurité au plus près des ressources et obtenir une visibilité réseau à l'échelle de l'entreprise. C'est un grand défi qui dépend de la microsegmentation : diviser le réseau en zones contenues, contrôler le mouvement entre elles et appliquer des exigences d'accès plus strictes pour les données et les systèmes à plus forte valeur ajoutée.

Un concept clé ici est la séparation des tâches (SOD). L'équipe réseau doit gérer le réseau pour obtenir les meilleures performances tandis que l'équipe de sécurité gère l'accès. Lorsqu'elles sont définies correctement, les stratégies de séparation des tâches permettent de s'assurer qu'aucune personne n'a le contrôle total sur un processus ou une transaction sensible. Il faut éviter à tout prix que l'administrateur réseau responsable de la création et de la gestion des comptes utilisateur dispose des droits d'accès permettant de supprimer des entrées de journal de sécurité, par exemple.

Pilier : Applications et workloads

L'approche zero trust concerne les applications et les workloads exécutés on-premises, sur les appareils mobiles et dans le cloud. CISA recommande d'intégrer des tests de sécurité tout au long du cycle de développement du logiciel et de nécessiter des tests automatisés de toutes les applications.

Les pratiques de développement natives du cloud contribuent à un modèle de sécurité zero trust, car ces applications modulaires utilisent une architecture de microservices et une conteneurisation, ce qui permet d'isoler les composants. Chaque service fonctionne indépendamment et dispose d'un accès minimal à d'autres services, sauf accord explicite.

Plus de **80 %** de toutes les violations de données d'aujourd'hui sont attribuées à une erreur ou à une négligence de la part de collaborateurs. En mettant en œuvre la zero trust, les entreprises peuvent limiter les dommages causés par des utilisateurs négligents.

Source : SANS Institute

Pilier : Données

La protection des données est l'une des principales raisons pour lesquelles les entreprises adoptent la zero trust, de sorte que ce pilier se rattache à trois domaines d'intérêt et améliore

- la disponibilité, en veillant à ce que les données soient accessibles quand et où elles sont nécessaires ;
- la confidentialité, en se protégeant contre tout accès non autorisé ;
- l'intégrité, en veillant à ce que les données ne soient pas altérées, perdues ou corrompues.

Dans le modèle CISA, les clés du succès incluent la catégorisation et l'étiquetage automatisés des données à l'échelle de l'entreprise, des stratégies robustes de prévention de la perte de données qui protègent contre le vol d'informations sensibles, un chiffrement puissant omniprésent et une révision continue des autorisations.

Souvent, les entreprises en appliquent déjà un grand nombre dans leurs bases de données. Les mesures doivent inclure le contrôle d'accès basé sur les rôles, le chiffrement transparent des données au repos et en transit, l'audit précis pour suivre et consigner l'activité des utilisateurs et les modifications apportées à la base de données, et les fonctionnalités de protection contre les exploits courants, tels que les attaques par injection SQL.

Enfin, les trois fonctionnalités transversales de CISA (visibilité et analyse, automatisation et orchestration, et gouvernance) s'étendent sur les cinq piliers.

La visibilité et l'analyse consistent à disposer des données appropriées pour éclairer les décisions stratégiques et répondre rapidement aux problèmes. L'automatisation et l'orchestration s'appuient sur ces données pour gérer les incidents de sécurité lorsqu'ils surviennent. Les capacités de gouvernance aident les organisations à gérer et à surveiller leurs exigences réglementaires, juridiques, environnementales, fédérales et opérationnelles pour soutenir la prise de décision basée sur le risque.

Réalités culturelles de la zero trust

La couche de gouvernance de CISA consiste également à avoir les bonnes personnes, les bons processus et les bonnes technologies. Une approche zero trust efficace nécessite que les trois travaillent de concert, de sorte que si votre modèle de sécurité réseau actuel accorde un niveau de mobilité entre actifs une fois que les utilisateurs sont à l'intérieur du réseau, la zero trust sera probablement un changement significatif.

Un point de blocage est souvent un nouvel accent mis sur les pratiques de gestion des identités et des accès, par exemple des stratégies de mot de passe plus strictes ou même l'élimination totale des mots de passe, l'authentification multifacteur et une approche plus centralisée de la gestion des identités et des privilèges d'accès des utilisateurs. Les personnes habituées à des contrôles plus lâches peuvent trouver ces changements gênants et la productivité peut effectivement chuter jusqu'à ce que les utilisateurs s'habituent au nouveau modèle.

La sécurité zero trust implique un examen plus minutieux de l'activité des utilisateurs et de la santé des appareils, ce qui peut agacer certains collaborateurs soucieux de leur vie privée qui estiment que leurs actions sont surveillées de trop près. Certains refuseront d'installer des logiciels mandatés sur leurs appareils personnels.

En outre, les professionnels de la sécurité, des opérations réseau et du développement d'applications ne sont pas à l'abri du ressentiment. Vous avez compris l'idée générale. C'est un changement radical où le succès dépend de l'adhésion des utilisateurs et d'un leadership exécutif solide.

Les stratégies pour une transition en douceur comprennent :

Une communication claire des raisons de l'adoption de la zero trust, en mettant l'accent sur les avantages commerciaux. Répondez ouvertement aux préoccupations de confidentialité des collaborateurs et expliquez comment la zero trust protège leurs données. Envisagez des formations et des sessions d'informations sur les principes et les bonnes pratiques de zero trust.

Un déploiement progressif qui donne aux collaborateurs, aux partenaires et au personnel informatique le temps de s'adapter. Donnez la priorité à l'implémentation d'une sécurité zero trust de manière à perturber au minimum les workflows et à maintenir une expérience utilisateur positive. Les technologies basées sur le cloud peuvent beaucoup aider dans ce cas de figure.

Une séparation claire des tâches au sein de l'organisation, dans le but d'empêcher les utilisateurs d'accéder aux ressources ou d'effectuer des actions en dehors des rôles qui leur sont affectés. Cela peut aider à prévenir les activités frauduleuses dans tous les services.

Le leadership salue les efforts des collaborateurs. Cette reconnaissance peut grandement faciliter la transition. Toutefois, les dirigeants doivent également faire de la sécurité zero trust une initiative stratégique et allouer suffisamment de ressources, travailler avec les équipes informatiques pour aligner les contrôles sur les objectifs de l'entreprise et insister sur des indicateurs clés de performance pour mesurer l'efficacité.

6 indicateurs de succès de l'approche zero trust

Dans un guide de stratégie publié récemment, le SANS Institute, un fournisseur mondial de formation et de certification en cybersécurité, liste six indicateurs clés pour mesurer l'efficacité de votre implémentation zero trust.

1. **Taux de succès d'authentification.** Mesure le pourcentage de tentatives d'authentification réussies par rapport au nombre total de tentatives.
2. **Taux de conformité aux règles.** Mesure le pourcentage de demandes d'accès conformes à vos stratégies de zero trust.
3. **Nombre de tentatives de mouvement latéral.** Mesure le nombre de tentatives de déplacement latéral détectées au sein du réseau après l'accès initial.
4. **Délai de détection et de réponse aux incidents** Mesure le temps moyen nécessaire pour détecter les incidents de sécurité et y répondre.
5. **Anomalies d'analyse des comportements des utilisateurs et des entités.** Mesure le nombre et la gravité des anomalies détectées dans les comportements des utilisateurs et des entités pour suivre les menaces potentielles à la sécurité.
6. **Retour des parties prenantes.** Collecte des données provenant de rôles techniques et non techniques dans tous les groupes, y compris les équipes interfonctionnelles, les utilisateurs finaux et les responsables d'équipe.

6 bonnes pratiques en matière d'architecture zero trust

CISA souligne que la plupart des grandes entreprises, y compris les gouvernements, sont confrontées à des défis communs avec les anciens systèmes, où l'accès et l'autorisation sont souvent basés sur des attributs fixes et rarement évalués. Sur le plan technologique, s'éloigner de cette structure obsolète nécessite des changements architecturaux.

Voici les principales bonnes pratiques :

1

Accès minuté et validé à l'aide d'une structure d'autorisation

Supposons qu'un employé se connecte le matin à l'aide d'un service d'autorisation, tel que OAuth, qui émet des jetons valides pour des systèmes spécifiques et une période limitée et qui remplace un mot de passe. Lorsqu'il a besoin d'accéder à une base de données, ses droits pour ce système sont confirmés par le code d'autorisation du jeton.

2

Microsegmentation permanente

Plus vous pouvez limiter les mouvements latéraux sans dégrader les performances, mieux c'est. CISA recommande des micropérimètres distribués et une microsegmentation étendue en fonction de la configuration de vos applications. Il n'est pas question de placer des pare-feu partout ; pour isoler et sécuriser les segments sans ralentir inutilement les flux de trafic, vous pouvez recourir à des techniques telles que les machines virtuelles pour chaque application, le chiffrement du trafic est-ouest, la création de réseaux définis par logiciel au sein du réseau physique et des algorithmes de routage intelligents.

3

Journalisation en fonction du contexte

L'IA peut jouer un rôle important ici via l'authentification adaptative basée sur des techniques d'évaluation des risques qui peuvent aider à détecter les anomalies et, en réponse, à relever les défis d'authentification. Vérifiez que vos fournisseurs ne se contentent pas d'analyser les journaux en temps réel pour identifier les anomalies et les menaces potentielles, mais qu'ils corrèlent aussi les événements pour repérer les modèles complexes qui pourraient signaler une attaque avancée.

4 Chiffrement omniprésent

Vos données constituent probablement votre ressource la plus critique. Leur protection au repos, en transit et en cours d'utilisation exige un chiffrement de bout en bout associé à une surveillance pour détecter les tentatives d'accès non autorisées.

5 Accès avec les moindres privilèges

Dans le contexte de la sécurité zero trust, le moindre privilège est un principe fondamental. Si vous limitez l'accès à ce qui est nécessaire pour les utilisateurs, les applications et les appareils, ce n'est pas par manque de confiance envers les collaborateurs, mais pour réduire les risques. Cette approche limite les dommages si un acteur malveillant parvenait à exploiter des informations d'identification volées, un périphérique compromis ou une vulnérabilité.

6 Un accent mis sur la fiabilité des appareils

La sécurité zero trust consiste à n'accorder aucune confiance inhérente à un appareil, même s'il se trouve à l'intérieur du périmètre, appartient à l'entreprise ou a déjà obtenu un accès. Pour gagner en confiance, il peut s'agir de répondre aux exigences de sécurité, telles que la mise à jour des logiciels, la protection antivirus et la surveillance.

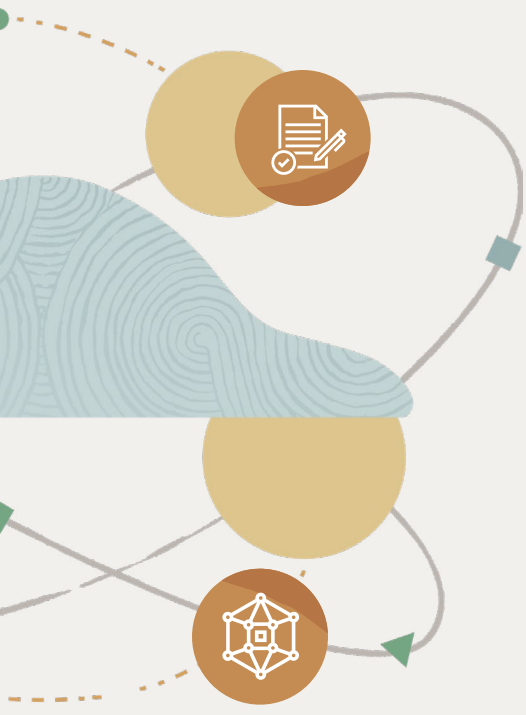
Vos utilisateurs ont tendance à prendre du retard sur la mise à jour de la version logicielle ou de la signature de logiciels malveillants ou à résister à l'installation de logiciels de sécurité sur leurs appareils personnels ? La sécurité zero trust leur forcera la main, car un appareil sans le profil de sécurité défini par votre stratégie se verra tout simplement refuser l'accès. Le service informatique doit gérer la sécurité des terminaux sur les appareils appartenant à l'entreprise et la conformité doit être vérifiée lors du lancement de nouvelles sessions.

Les fournisseurs de cloud et la sécurité zero trust

Les entreprises qui utilisent des services cloud peuvent commencer à mettre en œuvre la sécurité zero trust. Les hyperscalers offrent des solutions, des modèles et des outils de sécurité préconfigurés, permettant un déploiement plus rapide de contrôles zero trust et une meilleure évolutivité et une gestion centralisée.

En outre, de nombreux fournisseurs cloud ont adopté des fonctionnalités d'automatisation basées sur l'IA générative pour minimiser les erreurs humaines et aider les équipes des opérations de sécurité à configurer des contrôles qui tirent pleinement parti des fonctionnalités de sécurité natives fournies par les fournisseurs cloud, telles que les pare-feu, les systèmes de détection d'intrusion, le chiffrement, la vérification continue, l'accès avec le moindre privilège, la gestion du cycle de vie des identités et la microsegmentation.

Zero Trust Packet Routing (ZPR), un langage de stratégie basé sur les intentions qui permet aux administrateurs de définir des chemins d'accès aux données pour les ressources dans le cloud, est l'une des technologies clés permettant de soutenir les efforts de zero trust des fournisseurs cloud. Le trafic qui n'est pas explicitement autorisé par la stratégie ne peut pas traverser le réseau.



Avantages de ZPR :

Politiques lisibles écrites en langage naturel et faciles à comprendre, à auditer et à gérer.

Découplage de la sécurité réseau de l'architecture réseau, ce qui permet de réduire le risque d'erreur humaine et la complexité de la configuration.

Sécurité basée sur les intentions, ce qui signifie que ZPR utilise des attributs de sécurité pour identifier et organiser les ressources et les stratégies afin de contrôler l'accès à ces ressources.

Application des stratégies au niveau du réseau, indépendamment des modifications ou des erreurs de configuration de l'architecture réseau.

Parmi les autres technologies qui contribuent à la sécurité zero trust figurent l'accès réseau zero trust (ZTNA) et les courtiers en sécurité d'accès au cloud (CASB).

ZTNA, également connu sous le nom de périmètre défini par logiciel, est une approche de sécurité qui contrôle l'accès aux applications et aux ressources internes beaucoup plus précisément qu'un VPN traditionnel, qui accorde l'accès à un réseau entier une fois qu'un utilisateur est vérifié. ZTNA évalue les informations d'identification de sécurité chaque fois que l'accès à une ressource est demandé. Le système prend en compte le contexte et ne peut accorder qu'un accès partiel. Si l'accès est accordé, c'est via une session sécurisée entre l'entité requérante et la ressource spécifique. Ensuite, l'activité et l'état des périphériques sont surveillés en permanence pour détecter tout comportement anormal susceptible d'indiquer une menace.

Un CASB utilise le machine learning pour définir une référence de comportement standard pour chaque utilisateur en surveillant l'activité standard sur une période donnée. Le système utilise ensuite des analyses pour comparer en permanence le comportement par rapport à la ligne de base afin de détecter toute activité anormale pouvant indiquer un initié malveillant ou un compte compromis. L'informatique peut définir des règles sur le moment où suspendre le compte et quand déclencher une alerte pour le suivi.

Enfin, la gestion des droits d'infrastructure cloud (CIEM) se concentre sur la gestion des identités et de leurs droits d'accès dans les environnements cloud : IaaS, PaaS et SaaS. Recherchez les systèmes qui s'intègrent aux normes d'identité, tels que OAuth 2.0, SAML (Security Assertion Markup Language) et OpenID Connect, pour l'authentification et l'autorisation, et examinez les API proposées par vos fournisseurs cloud pour gérer les droits d'accès et le contrôle d'accès.

En fin de compte, la philosophie de zero trust « ne jamais faire confiance, toujours vérifier » devient rapidement la norme. Les entreprises qui s'accrochent à un état d'esprit de périmètre peuvent perdre la confiance des partenaires, des clients et des collaborateurs. Heureusement, vous pouvez trouver des modèles et de l'aide. Les fournisseurs de cloud donnent l'exemple.

Oracle Access Governance et zero trust

Oracle Access Governance permet une approche zero trust dans le cloud en fournissant une gouvernance complète des identités avec automatisation et contrôle d'accès de niveau fin. Il permet de s'assurer que l'accès est évalué en permanence et appliqué de manière dynamique en fonction du contexte et de la stratégie, en prenant en charge le principe « ne jamais faire confiance, toujours vérifier ».

Oracle Advanced Authentication, Oracle Adaptive Risk Management et Oracle Universal Authenticator offrent des fonctionnalités robustes pour mettre en place une architecture zero trust. Ces solutions proposent l'authentification multifacteur (MFA), la MFA résistante au phishing, l'authentification adaptative et la MFA au niveau de l'appareil avec des options sans mot de passe. Ensemble, ils fournissent des mesures de sécurité dynamiques qui s'adaptent au comportement des utilisateurs, à l'intégrité des appareils et aux risques contextuels, ce qui contribue à garantir un accès sécurisé aux ressources critiques.

En quoi Oracle peut-il vous aider ?

Avec l'approche axée sur la sécurité d'Oracle, des stratégies explicites sont requises pour l'accès à Oracle Cloud Infrastructure (OCI). Chaque composant est considéré comme une ressource au sein d'OCI et l'accès doit être spécifiquement accordé. Toutes les communications au sein d'OCI sont chiffrées et les droits d'accès sont vérifiés par rapport aux stratégies existantes. Ces stratégies peuvent être structurées de manière à octroyer un contrôle d'accès extrêmement précis pour chaque ressource, y compris l'implémentation d'un accès dynamique.

OCI implémente la surveillance et l'audit sur les ressources cloud, ce qui vous permet d'utiliser le stockage d'objets existant pour effectuer des analyses, ou vous pouvez utiliser l'outil de gestion des informations de sécurité et des événements de votre choix. Oracle Cloud Guard Instance Security fournit des réponses automatisées aux événements déclenchés, ce qui permet d'accélérer le temps de réaction aux menaces potentielles.

De plus, OCI Zero Trust Landing Zone permet désormais le provisionnement en un clic pour une architecture sécurisée et performante pour votre location cloud, avec le déploiement et la configuration renforcée des services clés nécessaires pour répondre à certaines exigences de zero trust.

En savoir plus

Restez en contact

En Canada, composez le +1 800 363 3059 ou visitez le site oracle.com/ca-fr/

En dehors de la Canada, trouvez votre bureau local à l'adresse oracle.com/ca-fr/corporate/contact/