Engineer

Zero trust

un modèle sans confiance fondée sur la seule position réseau

Ce que c’est

Le zero trust est un modèle de sécurité dans lequel rien n’est jugé fiable en raison de sa position sur le réseau. NIST SP 800-207, la publication fédérale américaine qui a exposé le modèle en 2020, le définit comme un paradigme centré sur la protection des ressources, selon le principe qu’aucune confiance n’est accordée implicitement et qu’elle doit être évaluée en permanence. Le seul fait d’être dans le réseau du bureau, sur le VPN ou dans le même centre de données ne confère aucun droit à une demande. Chaque demande d’accès à une ressource est évaluée pour elle-même : qui demande, depuis quel appareil, pour quoi faire et dans quelles conditions. En anglais, zero-trust avec un trait d’union qualifie un nom, comme dans « zero-trust design » ; le plan qui met le modèle en œuvre s’appelle une architecture zero trust, ou ZTA.

Le NIST nomme précisément les acteurs. Un sujet est celui ou ce qui émet une demande : un utilisateur, un service ou un appareil. Une ressource est tout ce qui mérite d’être protégé, et la publication compte les imprimantes et la capacité de calcul au même titre que les données. Trois composants logiques se placent entre les deux. Le moteur de politique décide si une demande est acceptée et consigne sa décision. L’administrateur de politique la met en œuvre : il ouvre ou ferme le chemin entre le sujet et la ressource et délivre les identifiants ou les jetons pour cette seule session. Le point d’application de la politique se trouve sur le trajet lui-même : il laisse passer la session, la surveille et y met fin lorsqu’on le lui demande.

La publication explique le changement par un aéroport. Les passagers passent un contrôle de sécurité, puis voyageurs, équipages et personnel de l’aéroport circulent dans le terminal, tous considérés comme fiables. Ce terminal est ce que le NIST appelle une zone de confiance implicite : une zone dans laquelle chacun

bénéficie du niveau de confiance du dernier contrôle passé. Un réseau de bureau plat fonctionne de la même manière. Le zero trust réduit cette zone autant que possible en rapprochant la décision et son application de la ressource.

Utilisez le concept pour prendre une décision

Utilisez « Qu'est-ce que le zero trust ? » pour éclairer une décision réelle. Nous pouvons vous aider à relier ce concept au système que vous construisez ou achetez. Des comptes, mots de passe et droits attribués selon les besoins exacts de chaque poste, puis retirés le jour du départ.

Découvrir nos prestations Contactez-nous →

Vérifiez les hypothèses derrière le terme

Appuyez-vous sur l'explication et les réalisations liées pour formuler les questions de votre projet. Nous pouvons examiner les hypothèses avec vous avant le choix d'un outil. 1 000 règles RBAC pour sécuriser Linux — 1,000 règles d'accès écrites pour combler une faille de sécurité

1 000 règles RBAC pour sécuriser Linux Contactez-nous →

Pourquoi c’est important

L’ancien modèle trace une limite autour de l’organisation et fait confiance à ce qui se trouve à l’intérieur. L’objection du NIST est claire : une fois le périmètre franchi par des attaquants, leurs déplacements latéraux ne sont plus entravés, et les déplacements latéraux non autorisés figurent parmi les plus grands problèmes des organismes auxquels la publication s’adresse. La limite ne correspond plus non plus au travail réel. Le personnel se connecte depuis les réseaux de domicile ou d’hôtel, les appareils personnels sont autorisés sur certains systèmes, et une grande partie des outils utilisés fonctionne dans le cloud d’un tiers. Les hypothèses du NIST en découlent : le réseau privé n’est pas une zone de confiance implicite, un attaquant peut déjà s’y trouver, et le personnel à distance devrait traiter comme hostile le réseau local depuis lequel il se connecte.

Ce qu’une équipe gagne, c’est le cloisonnement. Selon le troisième des sept principes du NIST, l’accès est accordé par session avec les seuls privilèges nécessaires à la tâche, et une authentification auprès d’une ressource ne confère aucun droit sur une autre. Un mot de passe volé ou un portable compromis n’atteint alors que ce que ce compte et cet appareil sont autorisés à atteindre, à cet instant et par un seul point d’application, plutôt que tout le réseau interne. Les décisions laissent aussi une trace. Le moteur de politique consigne chaque autorisation et chaque refus : la réponse à la question de savoir qui pouvait atteindre un système et pourquoi vient des journaux plutôt que des souvenirs.

À quoi cela ressemble en pratique

Prenons un système d'achats, le type d'application que le NIST suggère pour une première migration parce qu'un groupe défini de salariés l'utilise, contrairement à la messagerie dont dépend toute l'organisation. Un acheteur l'ouvre depuis un portable de l'entreprise. La demande atteint le point d'application de la politique placé devant l'application ; ce point interroge le moteur de politique. Son algorithme de confiance pondère les données que liste le NIST : la demande elle-même, dont la version du système d'exploitation de l'appareil et son niveau de correctifs ; la base des sujets ; la base des actifs ; les exigences propres à la ressource, qui peuvent indiquer un niveau d'assurance de l'authentification ou refuser des adresses étrangères ; et les renseignements sur les menaces. Un enregistrement de décision illustratif, dont les noms de champs sont les nôtres et non ceux d'un produit, pourrait se lire ainsi :

```
demande   buyer-17 sur laptop-0417 -> application d'achats, lecture et écriture
sujet     équipe des achats ; connexion par clé résistante au hameçonnage
actif     géré par l'entreprise, correctifs OS à jour, disque chiffré
ressource exige AAL2 ou plus, appareil géré et IP source du pays
menace    adresse source absente des flux de menaces consultés
décision  lecture et écriture accordées pour cette session ; journal : approuvé
```

L'autorisation ne couvre que cette session et cette application. Lorsque le même acheteur, sur le même portable, ouvre les contrats de fournisseurs conservés dans un espace documentaire, le moteur prend une nouvelle décision d'accès : l'authentification auprès de la première ressource n'accorde pas automatiquement l'accès à la seconde. Le contexte compte aussi. Un exemple du NIST est un comptable qui travaille normalement aux heures de bureau et demande soudain le système financier au milieu de la nuit depuis un lieu que le moteur ne reconnaît pas : un algorithme de confiance contextuel peut déclencher une alerte et exiger que le sujet atteigne d'abord un niveau de confiance plus strict. Un autre est un membre des ressources humaines qui consulte normalement 20 à 30 dossiers du personnel par jour, puis en demande plus de 100.

Pour les services cloud, le NIST indique que les clients peuvent atteindre le service directement, les points d'application de l'organisation vérifiant la politique sur le trajet, plutôt que d'entrer d'abord dans le réseau interne par un VPN. Chacune de ces décisions suppose une vision nette de qui doit pouvoir atteindre quoi. Le NIST demande donc un recensement des actifs, des sujets, des flux de données et des processus avant toute réalisation. Ce travail préalable

correspond au type de consolidation décrit dans notre étude sur la gestion des accès dans M365 et SSO : identités et accès réunis dans M365, 1Password, Red Hat SSO et OKTA SSO, moindre privilège appliqué et procédures d'arrivée et de départ standardisées pour que les accès soient accordés et révoqués rapidement.

Où les problèmes surviennent

L'acheter comme un produit. Le NIST précise que le zero trust est un ensemble de principes directeurs plutôt qu'une architecture unique, et qu'il n'existe pas d'ensemble unique d'outils ou de services pour une entreprise zero trust. Une nouvelle passerelle d'accès distant portant l'étiquette sur sa boîte change peu de chose si chaque sujet admis peut encore atteindre tout le réseau derrière elle. Correction : traitez la transition, selon les termes du NIST, comme « un parcours plutôt qu'un remplacement intégral », un processus métier à la fois. Évaluez chaque produit au regard des principes qu'il doit satisfaire, notamment la possibilité de passer plus tard chez un autre fournisseur avec ses formats de données.

Écrire la politique avant l'inventaire. Le moteur de politique ne peut décider qu'à partir de ce qu'il sait des sujets, des actifs et des processus. Lorsque ces connaissances sont incomplètes, avertit le NIST, le résultat habituel est un processus métier qui s'arrête parce que le moteur refuse des demandes faute d'informations. Le shadow IT, les systèmes mis en place hors de la gestion du service informatique, aggrave le problème. Correction : recensez et cataloguez d'abord les actifs, les sujets, les flux de données et les processus, shadow IT compris, puis seulement écrivez les critères d'un processus candidat.

Les administrateurs conservent un accès général. Dans beaucoup d'anciennes conceptions, les développeurs et les administrateurs système peuvent atteindre chaque ressource, et le NIST demande une surveillance accrue de ces comptes. Soumettre tous les autres utilisateurs à des décisions par session tout en laissant aux comptes d'administration leur accès permanent fait des identifiants les plus précieux le chemin d'entrée le plus court. Correction : faites passer les comptes privilégiés par le même moteur, donnez-leur les accès nécessaires à leur tâche actuelle et utilisez journaux et audits pour apprendre leurs comportements habituels afin que les écarts ressortent.

Le moteur de politique devient le nouveau périmètre. Aucune ressource ne communique avec une autre sans l'accord du moteur et de l'administrateur. Quiconque a accès aux règles du moteur peut effectuer des modifications non autorisées ou commettre de simples erreurs, et un attaquant qui perturbe les points d'application ou l'administrateur peut bloquer l'activité. Correction : consignez et auditez chaque changement de configuration, exécutez les mécanismes d'application dans un environnement cloud correctement sécurisé ou répliquez-les sur plusieurs sites. Appliquez aux données de trafic conservées et à la politique les restrictions d'accès les plus strictes, en réservant l'accès aux seuls comptes d'administration dédiés.

Tout imposer dès le premier jour. Peu d'ensembles de règles sont corrects dès le premier essai, et le NIST prévoit une phase de réglage pendant laquelle des demandes qui devraient aboutir sont refusées. Passer directement à une application stricte prive le personnel des accès nécessaires à son travail à chaque lacune de la politique. Correction : exécutez le nouveau processus quelque temps en mode de simple compte rendu. Accordez la plupart des demandes, comparez les journaux à la politique prévue et n'appliquez que les règles de base, par exemple le refus des demandes qui échouent au contrôle MFA ou proviennent d'adresses connues comme hostiles. Renforcez la politique une fois le comportement normal compris.

Prendre MFA pour la ligne d'arrivée. MFA réduit le risque lié à un mot de passe volé, mais le NIST rappelle qu'un attaquant possédant des identifiants valides, ou un membre malveillant de l'organisation, peut encore atteindre tout ce que le compte est autorisé à atteindre. Correction : limitez la portée de chaque compte et utilisez un algorithme de confiance contextuel qui pondère l'heure, le lieu et le volume, pour que des identifiants valides employés de manière inhabituelle déclenchent quand même une alerte.

Pour aller plus loin

- NIST SP 800-207, Zero Trust Architecture — publié en août 2020 : la définition, les sept principes, les composants logiques, les menaces et une feuille de route pour la migration.
- NIST SP 1800-35, Implementing a Zero Trust Architecture — le guide pratique du NIST publié en juin 2025, décrivant 19 exemples d'implémentation construits avec 24 collaborateurs.

- NIST SP 800-207A — publié en septembre 2023 : le contrôle d'accès des applications cloud natives sur plusieurs clouds, fondé sur des passerelles API, des proxys sidecar et des identités de service plutôt que sur des adresses réseau.
- NIST SP 800-63B-4 — les niveaux d'assurance de l'authentification que les exigences d'une ressource peuvent nommer, dont AAL3 impose la résistance au hameçonnage.

Glossaire

Choisissez selon vos contraintes réelles

Présentez le parcours de déploiement, les risques opérationnels et les personnes d'astreinte. Nous pouvons définir un changement avec des vérifications, une procédure de reprise et une responsabilité claire.

Consulter les tarifs Contactez-nous →

Rendez la terminologie concrète

Demandez comment « Qu'est-ce que le zero trust ? » s'applique à votre organisation. Un exemple concret tiré de votre système actuel suffit pour engager la discussion.

Découvrir nos prestations

welcome@engineer.company +45 50 10 61 84 Copenhague, Danemark

Emportez cette page avec vous

Fiche de contact

Créé avec soin et amour par D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Droit d'auteur © 2025 – aujourd'hui · Engineer ApS · Tous droits réservés.

Imprimé depuis https://engineer.company/fr/glossary/zero-trust/