AYI NEDJIMI Consultants

Zero Trust IAM : architecture centrée sur l'identité

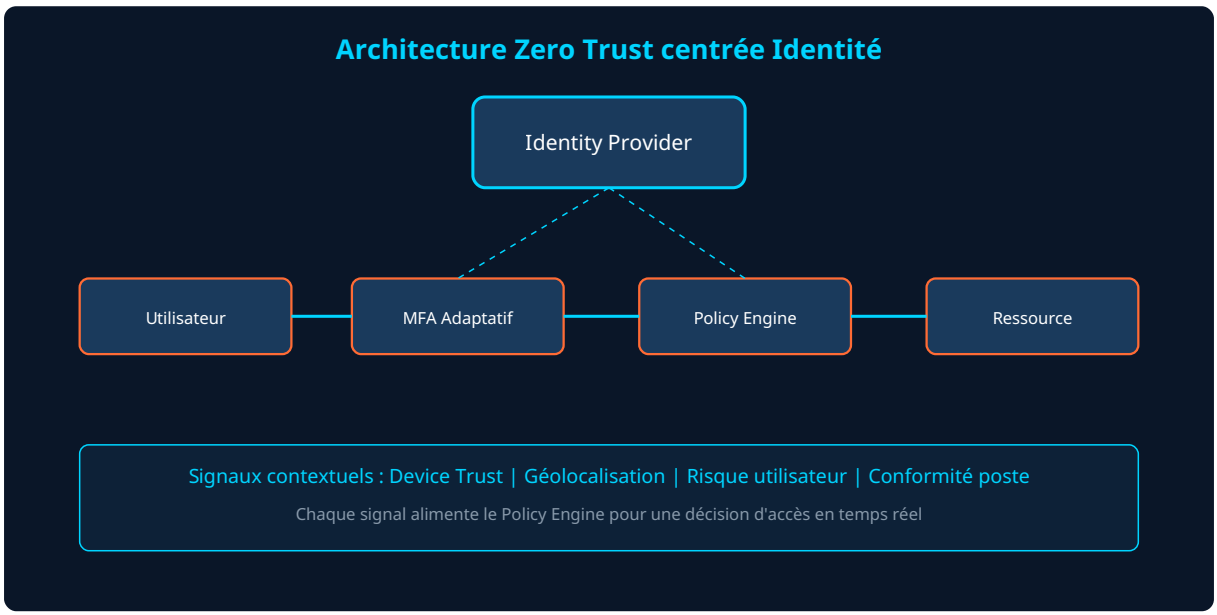
Catégorie : IAM et Gestion des Identités Lecture : 6 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Découvrez comment implémenter une architecture Zero Trust centrée sur l'identité avec IAM, MFA adaptatif et micro-segmentation pour protéger votre SI.

Le modèle Zero Trust a radicalement transformé la manière dont les entreprises abordent la sécurité de leur système d'information. Fini le périmètre réseau comme unique rempart : désormais, chaque requête, chaque connexion, chaque accès doit prouver sa légitimité. Et au centre de cette transformation se trouve l'identité. Que vous gériez un Active Directory on-premise, un tenant Entra ID ou un environnement hybride multi-cloud, l'architecture Zero Trust centrée sur l'identité redéfinit les règles du jeu. Ce guide vous accompagne dans la compréhension des principes fondamentaux, le choix des composants techniques et la mise en œuvre concrète d'une stratégie IAM Zero Trust. Nous aborderons les piliers architecturaux, les mécanismes d'authentification adaptative, la micro-segmentation basée sur les rôles et les retours d'expérience terrain qui font la différence entre une implémentation réussie et un projet enlisé. L'objectif est clair : vous donner une feuille de route actionnable, pas un discours théorique déconnecté du quotidien des équipes sécurité.

Points clés à retenir

- **Zero Trust** repose sur trois piliers : vérification explicite, moindre privilège, hypothèse de compromission
- L'identité remplace le périmètre réseau comme plan de contrôle principal
- Le **MFA adaptatif** et l'**accès conditionnel** sont les briques fondamentales de l'architecture
- La micro-segmentation par identité réduit la surface d'attaque latérale de 80% en moyenne
- Un déploiement progressif par vagues (pilote, critique, général) limite les risques de régression



Les trois piliers du Zero Trust appliqués à l'IAM

Le **NIST SP 800-207** définit trois principes fondateurs que toute architecture Zero Trust doit implémenter. Le premier, la vérification explicite, signifie que chaque demande d'accès est authentifiée et autorisée sur la base de tous les signaux disponibles : identité de l'utilisateur, état du terminal, localisation, sensibilité de la ressource. Le deuxième principe, le **moindre privilège**, impose de limiter l'accès au strict nécessaire avec des mécanismes de Just-In-Time et Just-Enough-Access. Le troisième, l'hypothèse de compromission, part du principe qu'un attaquant est déjà présent dans le réseau et segmente les accès pour minimiser le rayon d'explosion d'une brèche.

En pratique, ces trois piliers se traduisent par des composants techniques concrets. L'**Identity Provider** (IdP) devient le point de décision central. Les mécanismes de détection sur Entra ID permettent d'évaluer le risque en temps réel. Et les politiques d'accès conditionnel orchèstrent le tout avec une granularité fine.

Composants techniques d'une architecture Zero Trust IAM

Une architecture Zero Trust centrée identité s'articule autour de plusieurs briques complémentaires. L'*Identity Provider* (Entra ID, Okta, Ping Identity) gère l'authentification et la fédération. Le *Policy Decision Point* (PDP) évalue chaque requête selon les politiques définies. Le *Policy Enforcement Point* (PEP) applique la décision d'autorisation au niveau du réseau ou de l'application.

À ces composants s'ajoutent le **SIEM/XDR** pour la corrélation des signaux de risque, le **MDM/UEM** pour la conformité des terminaux et le coffre-fort de secrets pour la gestion des credentials programmatiques. L'ensemble forme un maillage où aucun composant ne fait confiance aux autres par défaut.

Composant	Rôle	Exemples
Identity Provider	Authentification, SSO, MFA	Entra ID, Okta, Ping
Policy Engine	Évaluation contextuelle des accès	Conditional Access, OPA
PAM	Accès privilégiés JIT	CyberArk, BeyondTrust, Delinea
ZTNA	Accès réseau zero trust	Zscaler, Cloudflare Access
MDM/UEM	Conformité des endpoints	Intune, Jamf, SCCM

Accès conditionnel et MFA adaptatif en pratique

L'accès conditionnel est le moteur de décision de votre architecture Zero Trust. Sur **Entra ID**, une politique d'accès conditionnel évalue cinq catégories de signaux : l'utilisateur (groupe, rôle, risque), l'application cible, le terminal (conformité, OS, ownership), la localisation (IP, pays) et le niveau de risque de la session (détection d'anomalies par Identity Protection).

Le risque lié aux attaques par mot de passe impose un MFA résistant au phishing pour les comptes sensibles. Les méthodes FIDO2 et Passkeys éliminent le vecteur d'attaque principal. Pour les populations moins exposées, le MFA par push notification avec number matching offre un bon compromis entre sécurité et ergonomie. La clé : adapter le niveau d'authentification à la sensibilité de l'opération demandée.

Micro-segmentation basée sur l'identité

La *micro-segmentation* traditionnelle repose sur des règles réseau (VLAN, pare-feu). La version Zero Trust va plus loin en segmentant par identité. Chaque utilisateur, chaque application, chaque **service account** se voit attribuer un périmètre d'accès dynamique qui évolue selon le contexte. Un administrateur qui se connecte depuis un poste non conforme verra ses privilèges réduits automatiquement, même si son compte est légitime.

L'intelligence artificielle appliquée à la micro-segmentation permet d'automatiser la création de ces périmètres en analysant les flux d'accès historiques. Les outils comme Illumio, Guardicore (Akamai) ou Azure NSG avec application security groups facilitent cette approche. Le gain est mesurable : selon Microsoft, les organisations ayant implémenté une micro-segmentation par identité réduisent leur surface d'attaque latérale de 80%.

Déploiement progressif : la méthode en trois vagues

Un déploiement Zero Trust IAM réussi ne se fait pas en big bang. La première vague cible un groupe pilote de 50 à 100 utilisateurs sur les applications les plus critiques. Vous activez le MFA, les politiques d'accès conditionnel en mode report-only, et vous mesurez l'impact. La deuxième vague étend le périmètre aux populations sensibles (admins, finances, RH) avec des politiques en mode enforcement. La troisième vague généralise à l'ensemble de l'organisation.

Chaque vague dure entre 4 et 8 semaines. Les métriques à suivre : taux de réussite MFA, nombre de blocages par politique, tickets support liés à l'authentification, et couverture des applications protégées. Un vCISO externalisé peut piloter ce déploiement pour les organisations qui manquent de ressources internes.

Intégration avec l'Active Directory existant

La majorité des entreprises ne partent pas d'une feuille blanche. L'**Active Directory** reste le socle identitaire pour 90% des grandes organisations. L'approche Zero Trust ne signifie pas remplacer l'AD du jour au lendemain, mais l'encapsuler dans une couche d'abstraction qui applique les principes Zero Trust. L'ANSSI recommande un modèle de tiering strict combiné à une synchronisation maîtrisée vers le cloud via Entra Connect.

Les attaques ciblant Active Directory exploitent souvent des chemins de compromission que le Zero Trust peut neutraliser. La suppression des accès directs RDP/SMB au profit de bastions PAM, le chiffrement Kerberos AES-256 exclusif et la surveillance des modifications LDAP sensibles sont des quick wins à fort impact.

Questions fréquentes sur le Zero Trust IAM

Combien de temps faut-il pour déployer une architecture Zero Trust IAM ?

Un déploiement complet prend généralement entre 12 et 24 mois selon la taille de l'organisation et la maturité existante. La phase pilote peut démarrer en 4 à 6 semaines. Les gains de sécurité sont progressifs : chaque vague réduit la surface d'attaque de manière mesurable. Les organisations de taille moyenne (500 à 2000 utilisateurs) atteignent typiquement une couverture de 80% en 9 mois.

Quel budget prévoir pour un projet Zero Trust centré identité ?

Le budget varie selon les briques existantes. Si vous disposez déjà de licences Microsoft E5, le surcoût se limite à l'intégration et au conseil (50 à 150 k€). Pour un environnement hétérogène nécessitant un IdP tiers et une solution PAM, comptez entre 200 et 500 k€ la première année, licences et services compris. Le ROI se mesure en réduction des incidents et en conformité réglementaire.

Le Zero Trust remplace-t-il le VPN traditionnel ?

Progressivement, oui. Le modèle ZTNA (Zero Trust Network Access) remplace le VPN en offrant un accès applicatif granulaire plutôt qu'un accès réseau large. Contrairement au VPN qui donne accès à un segment réseau entier, le ZTNA n'expose que les applications autorisées pour l'utilisateur authentifié. La transition se fait généralement en parallèle, le VPN restant actif pour les cas d'usage legacy.

Comment mesurer l'efficacité de son architecture Zero Trust ?

Quatre indicateurs clés : le pourcentage d'applications couvertes par l'accès conditionnel, le taux d'adoption du MFA résistant au phishing, le nombre de comptes à privilèges gérés par une solution PAM, et le temps moyen de détection d'une compromission d'identité (MTTD). Un tableau de bord centralisé dans votre SIEM permet de suivre ces métriques en continu.

Sources et références : ANSSI · MITRE ATT&CK

Synthèse et recommandations

L'architecture Zero Trust centrée sur l'identité n'est plus une option mais une nécessité face à l'évolution des menaces. Commencez par un audit de votre posture identitaire actuelle, identifiez les quick wins (MFA sur les comptes admins, suppression des accès permanents), puis déroulez votre feuille de route par vagues. Les outils existent, les méthodologies sont éprouvées. La vraie difficulté réside dans la conduite du changement et l'adhésion des métiers. Donnez-vous les moyens de réussir en impliquant les parties prenantes dès la phase de conception.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr