ManageEngine

LAZAR SOFT

Zero Trust by Design

ITCON

FRANCE 2026

Reprendre le contrôle de vos identités Active Directory.

01 · ORIGINES

Ni un produit. Ni du marketing.
Un modèle, né il y a trente ans.

1994

Stephen Paul Marsh

Université de Stirling, Écosse.

16 ans avant que le terme « Zero Trust » n'existe.

La confiance, formalisée comme un calcul

« Formalising Trust as a Computational Concept ».

Première tentative de mathématiser la confiance entre machines : des valeurs positives, négatives et nulles. La confiance à zéro naît ici, dans une thèse de doctorat.

Sa motivation : le ver Morris (1988), qui s'était propagé en exploitant les « trusted host connections » des machines se faisant aveuglément confiance.

La confiance devient une variable que l'on mesure. Donc une variable que l'on peut retirer.

Trente ans pour devenir un standard

1994
Stephen Marsh
Formalisation

2004
Jericho Forum
Dé-périmétrisation

2010
J. Kindervag
No More Chewy Centers

2021
Exec. Order 14028
Mandat fédéral US

Ni un produit, ni du marketing : un modèle architectural. **Standard NIST SP 800-207.**

ManageEngine

LA THÈSE

La confiance est difficile à donner.

Parce que l'humain change.
Et il change vite.

La conséquence

Pour atteindre le Zero Trust by Design, l'opérationnel doit quitter les mains de l'humain.

L'outil exécute : gain de temps, sécurité, réduction des erreurs.

« L'humain ne disparaît pas : il prend la direction et le contrôle. »

02 · LE PROBLÈME

Quand la faille porte un nom : L’humain.

Le périmètre s’est déplacé dans votre Active Directory. Et la plupart des incidents IAM ne viennent pas d’une attaque ciblée, ils viennent d’un geste humain, ou d’un geste oublié.

Trois failles, un seul coupable

01

Le compte qui survit au départ

Un collaborateur part, son compte reste. Comptes orphelins, accès jamais révoqués : c'est le scénario de l'« insider abuse », exactement le cas Cummings, 30 000 dossiers exfiltrés.

02

Le privilège qui s'accumule

À chaque mobilité, on ajoute des droits, on n'en retire jamais. Le moindre privilège théorique devient, en pratique, le privilège maximal. Personne ne nettoie.

03

L'erreur de la saisie manuelle

Provisionnement à la main : lenteur, fautes de frappe, droits copiés-collés d'un modèle obsolète. Chaque ligne tapée est un risque, et personne ne le trace.

Zero Trust + opérationnel humain = friction permanente

CE QUE LE ZERO TRUST EXIGE

- Vérification continue, à chaque accès
- Moindre privilège, strictement appliqué
- Révocation immédiate, sans délai
- Traçabilité totale de chaque action
- Cohérence parfaite, 24 h/24

CE QUE L'HUMAIN APPORTE

- De la latence : un ticket, une file d'attente
- De la fatigue et de l'incohérence
- Du turnover : il change, et change vite
- Des oublis : le départ non traité
- Aucune piste d'audit fiable

LE PIVOT

L’humain ne disparaît pas.

Il change de poste.

De l’exécution à la direction

On a longtemps demandé à l’humain de FAIRE : créer les comptes, attribuer les droits, désactiver, vérifier. C’est précisément là qu’il introduit délai, erreur et oubli.

Le bon rôle de l’humain n’est pas d’exécuter. C’est de décider, d’arbitrer, de définir la politique et de contrôler que l’outil l’applique.

L’IA audite.

L’outil opère.

L’humain pilote.

La nouvelle répartition des rôles

L'HUMAIN — il dirige

- Décide et arbitre
- Définit la politique d'accès
- Valide les exceptions
- Contrôle et supervise
- Lit l'audit, pas les logs

L'OUTIL & L'IA — ils opèrent

- Provisionnent et déprovisionnent
- Appliquent les droits à la lettre
- Journalisent chaque action
- Surveillent en continu
- Révoquent et alertent en temps réel

03 · L'ARSENAL MANAGEENGINE

Trois produits, trois rôles

ADManager Plus

L'OPÉRATIONNEL

L'outil exécute à la place de l'humain : Onboarding, Offboarding, gestion des droits, rapports, workflow de validation et l'ensemble sans erreurs.

ADAudit Plus

LE CONTRÔLE

L'IA au service de l'audit : surveillance continue, détection d'anomalies, d'attaques, de comportements suspicieux, vous êtes alertés. C'est ici que l'humain reprend la main.

ADSelfService Plus

L'AUTONOMIE

L'utilisateur se gère seul : mot de passe, MFA, déverrouillage. Zéro ticket, zéro intervention opérationnelle.

PILIER 1

ADManager Plus

L’opérationnel, automatisé.

La main qui crée et qui désactive n’est plus humaine.

L’outil prend l’opérationnel

Onboarding de masse : Créer 20, 200 ou 2 000 comptes depuis un modèle ou un fichier : en une opération.

Workflows d’approbation : La demande est humaine ; l’exécution est automatique et tracée.

Offboarding de masse: Le départ déclenche la révocation auprès de l’AD et des environnements M365 et Google Workspace.

Modèles & règles : Les droits viennent du rôle, pas d’un copier-coller d’un compte existant.

PILIER 2

ADAudit Plus

L’IA au service de l’audit.

C’est ici que l’humain reprend la direction : il contrôle, il ne tape plus.

L’humain dirige par l’audit

Surveillance continue : Chaque modification d’AD est captée en temps réel : qui, quoi, quand, où.

Détection d’anomalies : L’IA repère l’écart : élévation de privilège suspecte, connexion atypique.

Alertes & réaction : Le signal arrive au bon décideur ; la réponse peut être automatisée.

Conformité prête : Rapports NIS2, ISO 27001, RGPD générés en continu, pas en urgence d’audit.

La pleine autonomie de l’utilisateur

Réinitialisation en self-service : L’utilisateur regagne l’accès seul, sans ticket et sans appel au support.

MFA & déverrouillage : Sécurité renforcée et déblocage de compte gérés par l’utilisateur lui-même.

Mise à jour de profil : Coordonnées et attributs tenus à jour à la source, par l’intéressé.

L’IT déchargé : Moins d’opérationnel répétitif : le support se consacre à la valeur, pas aux mots de passe.

ManageEngine

PILIER 3

ADSelf Service Plus

L’utilisateur devient acteur de sa propre identité.

04 · LA DÉMONSTRATION

Et maintenant, un peu de magie.

ManageEngine

10 comptes. Créés, puis désactivés.

Le même geste, deux mondes — démonstration live sur AD Manager Plus.

À LA MAIN

- Des heures de saisie répétitive
- Une faute de frappe par lot, au moins
- Aucune traçabilité fiable
- Des comptes qu'on oubliera de fermer
- Un risque à chaque ligne

AVEC AD MANAGER PLUS

- Quelques minutes, pas quelques heures
- Zéro erreur : tout vient du modèle
- Chaque action est journalisée
- La désactivation est aussi rapide
- Le risque humain disparaît

La bascule Zero Trust by Design

L’outil exécute

Le provisionnement quitte les mains humaines.

L’humain dirige

Il décide, arbitre et contrôle la politique.

L’IA audite

Surveillance et anomalies en continu.

L’utilisateur est autonome

Il gère son identité, sans ticket.

ManageEngine

LAZAR SOFT

Merci.

Reprenez le contrôle de vos identités Active Directory et prenez rendez-vous avec nous :