International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.
© 2026 Scholar AI LLC.
https://ijpsat.org/
Vol. 59 No. 2 October 2026, pp. 735-748

Sécurité Des Identités Numériques Et Implémentation D'une Architecture Zero Trust Dans L'administration Des Réseaux

[Digital Identity Security And The Implementation Of A Zero Trust Architecture In Network Administration]

LOKULI LINGELE Alexandre[1], MPUTSHU BONYOMA Francis[1]

[1]Institut Supérieur Pédagogique de Mbandaka

Corresponding authors: LOKULI LINGELE Alexandre

(cc) BY

Résumé : La transformation des environnements numériques, caractérisée par l'essor du cloud computing, du télétravail, des objets connectés et des infrastructures distribuées, remet en question l'efficacité des modèles traditionnels de sécurité fondés sur la protection du périmètre réseau. Dans ce contexte, l'approche Zero Trust, fondée sur le principe « ne jamais faire confiance, toujours vérifier », constitue une réponse aux nouvelles menaces, particulièrement celles ciblant les identités numériques. Cette étude analyse la sécurité des identités numériques et l'implémentation d'une architecture Zero Trust dans l'administration des réseaux, en considérant l'identité comme un élément central du contrôle d'accès et de la gouvernance de la sécurité.

L'objectif de la recherche est de concevoir, d'évaluer et de proposer un cadre méthodologique permettant l'implémentation progressive d'une architecture Zero Trust centrée sur l'identité dans les environnements réseau d'entreprise. L'étude adopte une approche mixte, combinant une revue de la littérature, une analyse comparative des principaux frameworks et standards, notamment NIST SP 800-207, CISA ZTMM et les orientations de l'ANSSI, ainsi qu'une étude empirique fondée sur le déploiement et l'évaluation d'une architecture Zero Trust. L'architecture proposée intègre notamment la gestion des identités et des accès (IAM), l'authentification multifactorielle (MFA), les contrôles d'accès granulaires, la micro-segmentation, la vérification continue et la journalisation des activités.

Les résultats rapportés dans l'étude montrent une réduction de 73 % du nombre d'incidents de sécurité et une amélioration de 91 % du temps moyen de détection des incidents. Une forte corrélation positive (r = 0,85) est également observée entre la maturité des pratiques IAM et le taux de détection des intrusions. L'analyse qualitative souligne par ailleurs l'importance de l'implication de la direction, de la formation des administrateurs et des utilisateurs, d'une gouvernance structurée et d'une démarche d'implémentation progressive. Ces résultats soutiennent l'intérêt d'une architecture Zero Trust centrée sur l'identité pour renforcer les mécanismes de contrôle d'accès, améliorer la résilience des réseaux et réduire l'exposition aux menaces internes et externes. L'étude propose enfin des orientations opérationnelles pour une adoption progressive et contextualisée du Zero Trust, tenant compte des contraintes techniques, organisationnelles et budgétaires des entreprises.

Mots-clés : Sécurité des identités numériques ; Zero Trust ; administration réseau ; Identity and Access Management (IAM) ; authentification multifactorielle ; micro-segmentation ; contrôle d'accès ; cybersécurité.

Abstract: The transformation of digital environments, characterized by the growth of cloud computing, remote work, connected devices, and distributed infrastructures, challenges the effectiveness of traditional security models based on network perimeter protection. In this context, the Zero Trust approach, founded on the principle of "never trust, always verify," provides a response to emerging threats, particularly those targeting digital identities. This study analyzes digital identity security and the implementation of a Zero Trust architecture in network administration, considering identity as a central element of access control and security governance.

The objective of this research is to design, evaluate, and propose a methodological framework for the progressive implementation of an identity-centric Zero Trust architecture in enterprise network environments. The study adopts a mixed-method approach, combining a literature review, a comparative analysis of major frameworks and standards, including NIST SP 800-207, CISA ZTMM, and ANSSI guidelines, as well as an empirical study based on the deployment and evaluation of a Zero Trust architecture. The proposed

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.
© 2026 Scholar AI LLC.
https://ijpsat.org/
Vol. 59 No. 2 October 2026, pp. 735-748

architecture incorporates Identity and Access Management (IAM), Multi-Factor Authentication (MFA), granular access controls, network micro-segmentation, continuous verification, and activity logging.
The results reported in the study show a 73% reduction in the number of security incidents and a 91% improvement in the mean incident detection time. A strong positive correlation (r = 0.85) is also observed between the maturity of IAM practices and the intrusion detection rate. The qualitative analysis further highlights the importance of management involvement, administrator and user training, structured governance, and a progressive implementation approach. These findings support the relevance of an identity-centric Zero Trust architecture for strengthening access control mechanisms, improving network resilience, and reducing exposure to internal and external threats. Finally, the study proposes operational guidelines for the progressive and contextualized adoption of Zero Trust, taking into account the technical, organizational, and budgetary constraints of enterprises.

Keywords: Digital identity security; Zero Trust; network administration; Identity and Access Management (IAM); Multi-Factor Authentication; micro-segmentation; access control; cybersecurity.

I. Introduction

La transformation numérique a profondément changé la manière dont les organisations utilisent leurs systèmes informatiques et gèrent leurs réseaux. Le développement du cloud computing, du télétravail, des appareils mobiles et des objets connectés a rendu les infrastructures informatiques plus ouvertes et plus difficiles à protéger par les seules méthodes traditionnelles. Le fait d'être connecté au réseau interne ne suffit donc plus à garantir qu'un utilisateur ou un appareil est digne de confiance. Dans ce contexte, la gestion de l'identité numérique occupe une place de plus en plus importante dans la protection des ressources informatiques.

C'est dans cette évolution que s'inscrit l'approche **Zero Trust**, fondée sur un principe simple : **« ne jamais faire confiance, toujours vérifier »**. Contrairement au modèle traditionnel qui accorde généralement une certaine confiance aux utilisateurs se trouvant à l'intérieur du réseau, le Zero Trust exige que chaque demande d'accès soit vérifiée avant et pendant l'utilisation des ressources. Cette approche repose notamment sur une bonne gestion des identités et des accès, l'authentification multifactorielle, la limitation des privilèges, la micro-segmentation et la surveillance continue des activités.

La présente étude porte sur la **sécurité des identités numériques et l'implémentation d'une architecture Zero Trust dans l'administration des réseaux**. Elle cherche à comprendre comment l'identité peut devenir un véritable point de contrôle de la sécurité réseau et à proposer une démarche d'implémentation adaptée aux réalités des organisations. L'étude prend également en compte les contraintes techniques, organisationnelles et financières susceptibles d'influencer l'adoption de cette approche.

II. MATÉRIELS ET MÉTHODES

2.1. Matériels

2.1.1. Milieu d'étude

L'étude a été conduite dans trois organisations présentant des caractéristiques technologiques et organisationnelles différentes. Le choix de ces milieux repose sur leur diversité en matière de taille, de secteur d'activité, d'architecture informatique et de niveau de maturité technologique. Cette diversité permet d'examiner l'implémentation d'une architecture Zero Trust dans plusieurs contextes organisationnels.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.
© 2026 Scholar AI LLC.
https://ijpsat.org/
Vol. 59 No. 2 October 2026, pp. 735-748

Tableau 1. Caractéristiques des milieux d'étude

Organisation	Secteur	Taille	Infrastructure dominante	Particularités
Organisation A	Services financiers	500–1 000 employés	Hybride : *on-premise* et cloud	Maturité technologique avancée et exigences réglementaires élevées
Organisation B	Institution publique	> 1 000 employés	Principalement *on-premise*	Nombre élevé d'utilisateurs et contraintes budgétaires
Organisation C	Technologie	200–500 employés	Principalement cloud	Agilité technologique et expérience *cloud-native*

Source : Nos recherches.

2.1.2. Matériels et outils utilisés

La recherche a mobilisé différents outils pour l'analyse, la modélisation, la simulation et l'évaluation des architectures réseau. Les outils **Draw.io** et **Microsoft Visio** ont été utilisés pour représenter les architectures réseau et les différents composants de sécurité. Les environnements **GNS3** et **Cisco Packet Tracer** ont été utilisés pour la simulation et la validation des architectures Zero Trust proposées. L'étude a également pris en compte plusieurs composants technologiques associés au modèle Zero Trust, notamment la gestion des identités et des accès (IAM), l'authentification multifactorielle (MFA), le contrôle d'accès granulaire, la micro-segmentation, la vérification continue et la journalisation des événements de sécurité. Dans les différents cas étudiés, **Microsoft Entra ID**, **Keycloak**, **Okta Workforce Identity Cloud**, **Illumio**, ainsi que des mécanismes de contrôle et de détection adaptés aux différents environnements.

III. MÉTHODES

3.1. Approche et type de recherche

La recherche adopte une **approche méthodologique mixte**, combinant les méthodes qualitative et quantitative. L'approche qualitative a été retenue afin de comprendre les expériences des administrateurs réseau, les difficultés rencontrées lors de l'implémentation du Zero Trust, les perceptions des responsables de la sécurité ainsi que les réactions des utilisateurs face aux changements introduits dans les mécanismes d'accès.

L'approche quantitative a permis de mesurer les effets de l'implémentation de l'architecture Zero Trust à partir d'indicateurs techniques et de sécurité tels que le nombre d'incidents, le temps moyen de détection, le temps moyen de réponse, le taux de faux positifs, la couverture de l'authentification multifactorielle et le taux de conformité. L'étude s'inscrit également dans une démarche comparative à travers l'examen de trois contextes organisationnels différents et la confrontation des résultats aux principaux cadres de référence du Zero Trust, notamment ceux du **NIST, de la CISA et de l'ANSSI**.

3.2. Population et échantillon

3.2.1. Population d'étude

La population d'étude est constituée des acteurs directement impliqués dans l'administration des réseaux, la gestion des identités et la sécurité des systèmes d'information des organisations étudiées.

Elle comprend principalement :

- les administrateurs réseau ;
- les responsables de la sécurité des systèmes d'information (RSSI) ;
- les responsables des projets d'implémentation du Zero Trust ;
- les utilisateurs finaux.

Les architectures réseau existantes et les solutions de sécurité en place ont également été considérées comme des unités d'observation techniques.

3.2.2. Échantillon

L'étude a porté sur **25 participants** issus des trois organisations retenues. La sélection des participants a été réalisée de manière raisonnée, en privilégiant les personnes disposant d'une connaissance directe des systèmes réseau, de la gestion des identités, des mécanismes de contrôle d'accès et des pratiques de sécurité.

Tableau 2. Synthèse de l'échantillon et des unités d'observation

Élément	Description
Organisations étudiées	3
Participants	25
Administrateurs réseau / RSSI	Inclus dans l'échantillon
Responsables des projets Zero Trust	Inclus dans l'échantillon
Utilisateurs finaux	Inclus dans l'échantillon
Architectures réseau	Unités d'observation techniques
Solutions de sécurité	Unités d'observation techniques

Source : Nos recherches

La taille de l'échantillon constitue une limite de l'étude. Le support reconnaît que le nombre limité d'organisations et de participants réduit la possibilité de généraliser directement les résultats à l'ensemble des organisations.

3.3. Techniques et instruments de collecte des données

La collecte des données a reposé sur plusieurs techniques complémentaires.

3.3.1. Entretiens semi-directifs

Des entretiens semi-directifs ont été réalisés auprès des administrateurs réseau, des responsables de sécurité et des responsables des projets d'implémentation du Zero Trust.

Les entretiens ont principalement porté sur les pratiques de gestion des identités, les mécanismes d'authentification, les difficultés d'implémentation, les contraintes techniques et budgétaires, la résistance au changement et la perception de l'efficacité des solutions mises en place.

3.3.2. Observation

L'observation a permis d'examiner les pratiques existantes en matière d'administration réseau et de sécurité des systèmes d'information.

Elle a notamment porté sur les architectures réseau, les mécanismes de contrôle des accès, les solutions de sécurité déployées et les pratiques de gestion des identités.

3.3.3. Analyse documentaire

L'analyse documentaire a permis d'examiner les politiques, procédures, documents techniques et autres éléments disponibles dans les organisations étudiées.

Cette analyse a également été complétée par une comparaison avec les principaux cadres de référence du Zero Trust, notamment ceux du NIST, de la CISA et de l'ANSSI. [1]

3.3.4. Mesures quantitatives

Les mesures quantitatives ont porté sur plusieurs indicateurs permettant d'apprécier l'évolution de la posture de sécurité avant et après l'implémentation du Zero Trust. [5]

Tableau 3. Indicateurs retenus pour l'évaluation de l'architecture Zero Trust

Indicateur	Signification	Sens attendu après implémentation
Nombre d'incidents de sécurité	Nombre d'incidents observés par mois	Diminution
MTTD	Temps moyen de détection d'un incident	Diminution
MTTR	Temps moyen de réponse à un incident	Diminution
Taux de faux positifs	Proportion des alertes incorrectes	Diminution
Couverture MFA	Proportion des comptes protégés par MFA	Augmentation
Taux de conformité	Niveau de conformité aux politiques de sécurité	Augmentation

Ces indicateurs sont explicitement utilisés dans le support pour évaluer les performances de l'architecture proposée.

3.4. Modélisation et simulation

La modélisation des architectures réseau a été réalisée à l'aide de **Draw.io** et **Microsoft Visio**. Ces outils ont permis de représenter les différents composants de l'architecture Zero Trust et leurs relations.

La simulation des architectures a été réalisée avec **GNS3** et **Cisco Packet Tracer**, afin de visualiser et de valider les configurations proposées.

La conception s'est principalement articulée autour des mécanismes suivants :

- gestion des identités et des accès (IAM) ;
- authentification multifactorielle (MFA) ;
- contrôle d'accès basé sur les rôles ou le contexte ;
- principe du moindre privilège ;
- micro-segmentation ;
- vérification continue ;
- journalisation et audit ;
- surveillance des activités et détection des anomalies.

Cette organisation permet de placer l'identité numérique au centre du dispositif de contrôle d'accès, conformément à l'orientation **Identity-Centric Zero Trust** retenue dans la recherche.

3.5. Procédure d'expérimentation

L'expérimentation a été organisée autour de l'analyse de la situation initiale, de l'implémentation progressive des mécanismes Zero Trust et de l'évaluation des performances.

Dans l'Organisation A, l'approche a notamment commencé par la mise en place d'une solution IAM et de l'authentification multifactorielle, suivie de la micro-segmentation et de mécanismes de détection continue.

Dans l'Organisation B, compte tenu des contraintes budgétaires et de l'infrastructure principalement locale, l'implémentation a été progressive et s'est appuyée notamment sur une solution IAM open source ainsi que sur une micro-segmentation ciblée.

Dans l'Organisation C, l'environnement cloud-native a favorisé l'utilisation d'une solution IAM cloud et d'une solution d'accès réseau Zero Trust (ZTNA).

Les tests ont porté sur quatre dimensions principales :

1. **tests fonctionnels**, pour vérifier le fonctionnement des différents modules ;
2. **tests de performance**, pour mesurer les temps de réponse, la capacité de charge et la disponibilité ;
3. **tests de sécurité**, notamment à travers des simulations de phishing, de force brute et d'usurpation d'identité ;
4. **tests d'acceptabilité**, destinés à recueillir les perceptions des utilisateurs et des administrateurs.

3.6. Traitement et analyse des données

Les données qualitatives issues des entretiens, des observations et de l'analyse documentaire ont fait l'objet d'une **analyse thématique**. Cette analyse a permis d'identifier les principaux facteurs techniques, organisationnels et humains associés à la réussite de l'implémentation du Zero Trust.

Les données quantitatives ont été organisées autour des indicateurs de sécurité définis précédemment.

Tableau 4. Organisation du traitement des données

Type de données	Source	Méthode d'analyse	Finalité
Qualitatives	Entretiens	Analyse thématique	Identifier les facteurs, difficultés et perceptions
Qualitatives	Observations	Analyse descriptive	Examiner les pratiques et architectures
Documentaires	Politiques et documents techniques	Analyse documentaire	Comparer les pratiques aux référentiels
Quantitatives	Indicateurs de sécurité	Analyse statistique	Mesurer les effets du Zero Trust
Techniques	Simulations et tests	Analyse comparative	Évaluer la sécurité et les performances

L'analyse quantitative a notamment utilisé le **test t pour échantillons appariés** afin d'examiner les différences entre les mesures effectuées avant et après l'implémentation. Le support rapporte des différences statistiquement significatives avec un seuil de $\mathbf{p < 0,01}$.

Une analyse de corrélation a également été utilisée pour examiner la relation entre la maturité des pratiques de gestion des identités et le taux de détection des intrusions. Le document rapporte une corrélation positive de $\mathbf{r = 0,85}$.

3.7. Validité, fiabilité et triangulation

La validité interne de l'étude a été renforcée par la triangulation des différentes sources de données. Les informations provenant des entretiens, des observations et des mesures quantitatives ont été confrontées afin de renforcer la cohérence des résultats. La validité externe repose notamment sur la diversité des organisations étudiées en termes de secteur, de taille et de technologie, ainsi que sur la comparaison des résultats avec les travaux antérieurs.

La fiabilité a été recherchée à travers :

- la standardisation des procédures de collecte ;
- la formation des chercheurs aux techniques d'entretien et d'observation ;
- l'utilisation d'outils de transcription et d'analyse ;
- la documentation systématique des procédures et décisions méthodologiques.

La triangulation a été réalisée à trois niveaux :

Tableau 5. Dispositif de triangulation

Niveau	Principe
Triangulation des données	Croisement des données qualitatives et quantitatives provenant de plusieurs sources
Triangulation des méthodes	Combinaison des entretiens, observations, analyses documentaires et mesures quantitatives
Triangulation des chercheurs	Validation croisée des analyses par plusieurs membres de l'équipe

3.8. Considérations éthiques et gestion des données

La recherche a respecté les principes fondamentaux applicables aux études impliquant des participants et aux travaux de cybersécurité. Le consentement éclairé des participants a été obtenu après leur information sur les objectifs de l'étude, les méthodes utilisées et l'utilisation prévue des données. Les informations permettant d'identifier les participants et les organisations ont été anonymisées.

La participation était volontaire et les participants pouvaient se retirer de l'étude. Les tests de sécurité ont été réalisés dans des environnements contrôlés et avec l'autorisation des organisations concernées. Les données ont été stockées sur des serveurs sécurisés avec des accès restreints et des sauvegardes régulières. Le support prévoit également la conservation des données pendant cinq années après la publication des résultats.

3.9. Synthèse du dispositif méthodologique

Tableau 6. Synthèse de la méthodologie de recherche

Élément	Dispositif retenu
Type de recherche	Recherche empirique à approche mixte
Approche	Qualitative et quantitative
Milieu	Trois organisations de profils différents
Échantillon	25 participants
Unités d'observation	Administrateurs, RSSI, responsables Zero Trust, utilisateurs, architectures et solutions de sécurité
Techniques	Entretiens, observation, analyse documentaire, mesures quantitatives, simulations
Modélisation	Draw.io, Visio
Simulation	GNS3, Cisco Packet Tracer
Composants étudiés	IAM, MFA, contrôle d'accès, micro-segmentation, vérification continue, journalisation
Analyse qualitative	Analyse thématique
Analyse quantitative	Statistiques descriptives, test t apparié, corrélation
Validation	Triangulation des données, méthodes et chercheurs
Éthique	Consentement, anonymisation, volontariat, non-malfaisance
Gestion des données	Stockage sécurisé, accès restreint, sauvegarde et conservation

Source : Nos recherches.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.
© 2026 Scholar AI LLC.
https://ijpsat.org/
Vol. 59 No. 2 October 2026, pp. 735-748

IV. RÉSULTATS ET DISCUSSION

4.1. Résultats

4.1.1. Résultats des études de cas

L'étude a porté sur trois organisations présentant des environnements technologiques différents : une entreprise de services financiers disposant d'une infrastructure hybride, une institution publique principalement *on-premise* et une entreprise technologique reposant principalement sur le cloud. L'analyse a permis d'observer les conditions d'implémentation du Zero Trust, les difficultés rencontrées et les résultats obtenus dans chaque contexte.

4.1.2. Résultats de l'Organisation A : entreprise de services financiers

L'Organisation A disposait d'une infrastructure hybride associant des applications anciennes hébergées localement et des services cloud. L'audit initial a mis en évidence une surface d'attaque importante, des privilèges d'accès excessifs et une visibilité limitée sur les flux réseau.

L'implémentation du Zero Trust a commencé par le déploiement d'une solution de gestion des identités et des accès (IAM), **Microsoft Entra ID**, accompagnée de l'authentification multifactorielle (MFA). Une solution de micro-segmentation, **Illumio**, a ensuite été utilisée afin de limiter les mouvements latéraux, puis un système de détection et de réponse aux menaces a été intégré pour assurer une vérification continue.

Après douze mois d'implémentation, les résultats rapportés sont les suivants :

Tableau 7. Résultats obtenus dans l'Organisation A

Indicateur	Résultat
Réduction des incidents de sécurité	75 %
Amélioration du MTTD	90 %
Taux de conformité	95 %

Les administrateurs réseau ont également signalé une amélioration de la visibilité sur le réseau ainsi qu'une réduction de la charge de travail liée à la gestion des incidents.

4.1.3. Résultats de l'Organisation B : institution publique

L'Organisation B était caractérisée par une infrastructure principalement *on-premise*, un nombre important d'utilisateurs et des contraintes budgétaires importantes. Les principaux problèmes identifiés concernaient la gestion des droits d'accès, la résistance au changement et les ressources limitées disponibles pour une implémentation complète du Zero Trust. Une approche progressive a donc été adoptée. Une solution IAM open source, **Keycloak**, a été déployée pour centraliser la gestion des identités. Une micro-segmentation réseau de base a ensuite été mise en œuvre afin de protéger les données les plus sensibles. Une attention particulière a également été accordée à la sensibilisation et à la formation des utilisateurs.

Après neuf mois d'implémentation, les résultats rapportés sont les suivants :

Tableau 8. Résultats obtenus dans l'Organisation B

Indicateur	Résultat
Réduction des incidents de sécurité	60 %
Amélioration du MTTD	80 %
Taux de conformité	85 %

Ces résultats montrent une amélioration de la sécurité malgré les contraintes techniques, financières et organisationnelles propres à cette organisation. Le rôle de la formation et de l'accompagnement des utilisateurs a été particulièrement souligné dans le support de recherche.

4.1.4. Résultats de l'Organisation C : entreprise technologique

L'Organisation C disposait d'une infrastructure principalement cloud-native et d'une culture technologique avancée. Les principales difficultés concernaient la sécurisation des accès aux applications SaaS, la gestion des identités des partenaires externes et le respect des exigences relatives à la protection des données. L'implémentation s'est appuyée sur **Okta Workforce Identity Cloud** pour la gestion des identités et sur une solution **ZTNA** pour sécuriser les accès distants aux ressources.

Après six mois d'implémentation, les résultats rapportés sont les suivants :

Tableau 9. Résultats obtenus dans l'Organisation C

Indicateur	Résultat
Réduction des incidents de sécurité	80 %
Amélioration du MTTD	92 %
Taux de conformité	98 %

Les utilisateurs ont également rapporté une expérience d'accès aux ressources plus fluide et plus sécurisée.

4.2. Évaluation globale des performances

L'évaluation globale a comparé plusieurs indicateurs de sécurité avant et après l'implémentation du Zero Trust.

Tableau 10. Comparaison des indicateurs de sécurité avant et après l'implémentation du Zero Trust

Indicateur	Avant ZT	Après ZT	Variation
Incidents de sécurité / mois	15	4	−73 %
Temps moyen de détection (MTTD)	120 min	10 min	−91 %
Temps moyen de réponse (MTTR)	240 min	30 min	−87 %
Taux de faux positifs	25 %	5 %	−80 %
Couverture MFA	40 %	100 %	+150 %*
Taux de conformité	55 %	95 %	+72 %

La variation de la couverture MFA est exprimée selon le calcul présenté dans le support ; en termes de points de pourcentage, elle correspond à une progression de 60 points, de 40 % à 100 %. Ces résultats indiquent une amélioration globale des indicateurs étudiés après l'implémentation de l'architecture Zero Trust. Le nombre d'incidents passe de 15 à 4 par mois, tandis que le temps moyen de détection passe de 120 à 10 minutes. Le temps moyen de réponse diminue également de 240 à 30 minutes. L'augmentation de la couverture MFA, qui passe de 40 % à 100 %, traduit une généralisation de l'authentification multifactorielle dans l'environnement étudié. Le taux de conformité progresse quant à lui de 55 % à 95 %.

4.2.1. Analyse statistique

L'analyse statistique présentée dans le support a utilisé des tests t pour échantillons appariés afin d'examiner les différences entre les mesures réalisées avant et après l'implémentation du Zero Trust. Les améliorations observées sont rapportées comme statistiquement significatives avec $\mathbf{p < 0,01}$. Une analyse de corrélation a également mis en évidence une relation positive importante entre la maturité des pratiques de gestion des identités et le taux de détection des intrusions, avec $\mathbf{r = 0,85}$. Ce résultat soutient l'hypothèse selon laquelle la qualité de la gestion des identités constitue un facteur important de l'efficacité d'une architecture Zero Trust.

4.3. Évaluation qualitative

L'analyse des entretiens réalisés auprès des administrateurs réseau et des responsables de la sécurité a permis d'identifier plusieurs facteurs associés à la réussite de l'implémentation du Zero Trust.

4.3.1. Implication de la direction

Le soutien de la direction apparaît comme un facteur important dans la mise en œuvre du Zero Trust. L'engagement de la direction facilite notamment la mobilisation des ressources financières, humaines et techniques nécessaires au projet.

4.3.2. Formation et sensibilisation

La formation des administrateurs et la sensibilisation des utilisateurs constituent également des éléments importants. L'expérience de l'Organisation B montre notamment que l'accompagnement des utilisateurs a contribué à réduire les difficultés liées à la résistance au changement.

4.3.3. Approche progressive

Les résultats des trois organisations montrent l'intérêt d'une implémentation progressive. L'approche consiste à commencer par les composants les plus critiques, notamment l'IAM et la MFA, avant de déployer progressivement des mécanismes plus complexes tels que la micro-segmentation et la vérification continue.

4.3.4. Gouvernance de la sécurité

La gouvernance apparaît également comme un facteur important. La mise en place d'une structure de gouvernance, de mécanismes de suivi et de procédures régulières de révision des politiques contribue à maintenir les mesures de sécurité dans le temps.

4.4. Discussion

Les résultats obtenus montrent que l'implémentation d'une architecture Zero Trust centrée sur l'identité peut s'accompagner d'une amélioration importante de plusieurs indicateurs de sécurité. La diminution de 73 % des incidents et l'amélioration de 91 % du temps moyen de détection constituent les principaux résultats quantitatifs rapportés par l'étude.

4.4.1. Zero Trust et réduction des incidents de sécurité

La diminution du nombre d'incidents, de 15 à 4 par mois, suggère que le renforcement des mécanismes d'authentification, de contrôle d'accès, de segmentation et de surveillance peut contribuer à réduire l'exposition aux menaces. Ce résultat est cohérent avec les observations réalisées dans les trois organisations, bien que l'ampleur des améliorations varie selon le contexte. L'Organisation A enregistre une réduction de 75 %, l'Organisation B de 60 % et l'Organisation C de 80 %.

Ces différences montrent que l'efficacité du Zero Trust ne dépend pas uniquement des technologies utilisées. Elle semble également liée au niveau de maturité technologique, aux ressources disponibles, à la culture de sécurité et aux caractéristiques de l'environnement informatique.

4.4.2. Importance de la gestion des identités

La corrélation **r = 0,85** observée entre la maturité de l'IAM et le taux de détection des intrusions renforce l'importance accordée à l'identité numérique dans le modèle étudié.

L'identité ne constitue donc pas seulement un mécanisme d'authentification. Elle devient un élément central dans la décision d'accès aux ressources, notamment lorsque celle-ci est associée à la MFA, au principe du moindre privilège, au contrôle contextuel et à la vérification continue.

4.4.3. Importance du contexte organisationnel

La comparaison des trois organisations montre que le même principe Zero Trust doit être adapté au contexte de chaque organisation. L'Organisation A disposait de ressources technologiques relativement importantes et d'une infrastructure hybride. L'Organisation B devait composer avec des contraintes budgétaires et une infrastructure principalement locale. L'Organisation C bénéficiait quant à elle d'un environnement cloud-native et d'une culture technologique favorable.

Cette diversité confirme l'intérêt d'une démarche progressive et contextualisée plutôt que d'une reproduction uniforme d'une architecture Zero Trust.

4.4.4. Validation des hypothèses

Les résultats permettent de confronter les observations aux hypothèses formulées dans l'étude.

Tableau 11. Synthèse de la vérification des hypothèses

Hypothèse	Élément de vérification	Résultat rapporté
H1 : le Zero Trust centré sur l'identité réduit la surface d'attaque et le temps de compromission	Réduction des incidents et amélioration du MTTD	Soutenue par les résultats
H2 : son efficacité dépend de la maturité de l'IAM	Corrélation IAM–détection des intrusions : r = 0,85	Soutenue par les résultats
H3 : une implémentation progressive favorise une adoption durable	Retours des trois organisations	Soutenue par les observations
H4 : une gouvernance structurée renforce les effets du Zero Trust	Résultats et observations organisationnelles	Soutenue par les résultats

Les résultats rapportés dans le support soutiennent ainsi les quatre hypothèses initiales, tout en montrant que leurs effets doivent être interprétés en tenant compte du contexte propre à chaque organisation.

4.4.5. Comparaison avec les travaux antérieurs

Les résultats de cette recherche sont présentés dans le support comme étant globalement cohérents avec les travaux antérieurs consacrés au Zero Trust. L'étude cite notamment les travaux d'Adahman (2022), qui mettent en évidence les conséquences économiques de la non-implémentation du Zero Trust, ainsi que ceux de Silva (2026), qui rapportent une réduction de 76 % des violations dans un contexte Zero Trust.

La contribution particulière de la présente recherche réside dans l'importance accordée à **l'identité numérique comme pivot de l'architecture Zero Trust**, plutôt que de la considérer comme un composant secondaire parmi les autres mécanismes de sécurité.

4.5. Limites des résultats

L'interprétation des résultats doit tenir compte de plusieurs limites. Premièrement, l'étude repose sur un nombre limité d'organisations et de participants, ce qui réduit la possibilité de généraliser les résultats à l'ensemble des organisations. Deuxièmement, la durée d'observation, comprise entre six et douze mois selon les cas, ne permet pas d'évaluer les effets à long terme de l'architecture Zero Trust. Troisièmement, certaines solutions commerciales utilisées dans les cas étudiés, notamment Microsoft Entra ID, Okta et Illumio, peuvent ne pas être accessibles aux organisations disposant de ressources financières limitées.

Enfin, les différences de taille, de secteur d'activité et de maturité technologique entre les organisations limitent la transférabilité directe des résultats d'un contexte à un autre.

V. CONCLUSION

Cette étude avait pour objectif d'analyser la sécurité des identités numériques et l'implémentation d'une architecture Zero Trust dans l'administration des réseaux. L'approche mixte adoptée a permis d'examiner les effets de plusieurs mécanismes, notamment la gestion des identités et des accès (IAM), l'authentification multifacteur, la micro-segmentation, le contrôle des accès et la vérification continue.

Les résultats obtenus montrent une amélioration significative de la sécurité après la mise en œuvre de ces mécanismes. Le nombre d'incidents est passé de 15 à 4 par mois, le temps moyen de détection de 120 à 10 minutes et le temps moyen de résolution de 240 à 30 minutes. La couverture de l'authentification multifacteur a atteint 100 %, tandis que le niveau de conformité est passé de 55 % à 95 %. Une forte corrélation (r = 0,85) a également été observée entre la maturité de la gestion des identités et la capacité de détection des intrusions.

Ces résultats soulignent que la sécurité de l'identité constitue un élément central de l'approche Zero Trust. Toutefois, son efficacité dépend également du contexte technologique, de la gouvernance, de la formation des utilisateurs et d'une mise en œuvre progressive. Malgré les limites liées au nombre d'organisations étudiées et à la durée d'observation, cette recherche montre l'intérêt d'une approche Zero Trust adaptée aux réalités et aux capacités de chaque organisation.

RÉFÉRENCES

[1]. ANSSI. (2022). *Guide d'implémentation Zero Trust pour les Opérateurs d'Importance Vitale (OIV)*. Paris : ANSSI.

[2]. CISA. (2023). *Zero Trust Maturity Model, Version 2.0*. Cybersecurity and Infrastructure Security Agency.

[3]. CLOUD SECURITY ALLIANCE. (2013). *Software-Defined Perimeter (SDP) Specification*. Cloud Security Alliance.

[4]. GARTNER. (2019). *Secure Access Service Edge (SASE)*. Gartner.

[5]. IBM. (2024). *What is Zero Trust Implementation*. IBM.

[6]. KINDERVAG, J. (2010). *No More Chewy Centers: The Zero Trust Model of Information Security*. Forrester Research.

[7]. NIST. (2017). *Digital Identity Guidelines (SP 800-63)*. National Institute of Standards and Technology.

[8]. NIST. (2020). *Zero Trust Architecture (SP 800-207)*. National Institute of Standards and Technology.

[9]. ROSE, S., BORCHERT, O., MITCHELL, S. & CONNELLY, S. (2020). *Zero Trust Architecture*. NIST Special Publication 800-207.

[10]. ROUSSEAU, D. M., SITKIN, S. B., BURT, R. S. & CAMERER, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, 23(3).

[11]. KANG, H., LIU, G., WANG, Q., MENG, L. & LIU, J. (2023). Theory and application of Zero Trust security: A brief survey. *Entropy*, 25(12), 1595.

[12]. GAMBO, M. L. & ALMULHEM, A. (2025). Zero Trust Architecture: A systematic literature review. *arXiv*, 2503.11659.

[13]. MILES, M. B., HUBERMAN, A. M. & SALDAÑA, J. (2014). *Qualitative Data Analysis*. Thousand Oaks: Sage.

[14]. NORTHCUTT, S. & NOVAK, N. (2001). *Network Intrusion Detection*. Indianapolis: New Riders.

[15]. ISO/IEC. (2022). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection*. International Organization for Standardization.