2025

IN CYBER
FORUM
EUROPE

ZERO TRUST

LE NOUVEAU PARADIGME

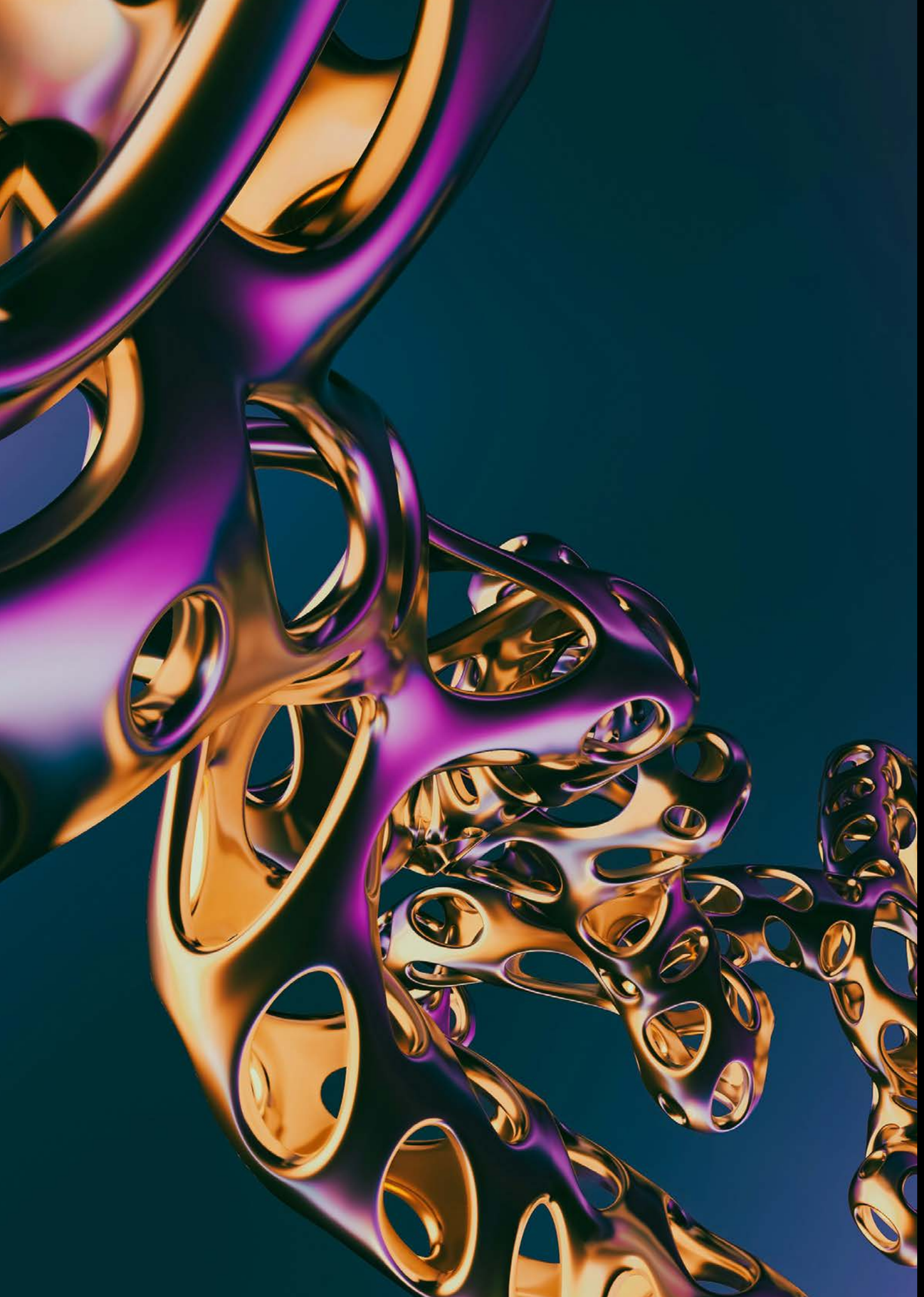
#INCYBERFORUM

en partenariat avec

CESIN

europe.forum-incyber.com

SOMMAIRE



ÉDITO

POURQUOI LE *ZERO TRUST* ?

Selon le dictionnaire, la confiance se définit comme « l'espérance ferme, l'assurance d'une personne qui se fie à quelque chose ou à quelqu'un ».

Dans le monde relationnel, c'est-à-dire l'ensemble des interactions et liens que nous tissons avec les autres, que cela soit dans un cadre professionnel ou personnel, la confiance est la plupart du temps implicite et basée sur une impression, un sentiment, une émotion. Elle est donc par définition incertaine… C'est à la fois sa beauté mais aussi sa fragilité. *A fortiori* dans un monde de plus en plus transactionnel, où les relations entre les individus et les organisations sont souvent dématérialisées. Alors que les échanges, qui sont autant de transactions, se multiplient, en particulier grâce à l'essor des technologies numériques, la confiance doit devenir explicite, mesurable, rationnelle, standardisée. Et donc être basée sur des garanties qui permettent de réduire au maximum l'incertitude.

La multiplication de ces échanges contribue également à l'émergence d'un monde de plus en plus ouvert et global, où les organisations sont dites « étendues ». Chacune devient un *hub* multipliant les transactions avec des acteurs externes. Et l'essor du *cloud computing,* le développement du télétravail et l'irruption de l'IA accélèrent encore la tendance : les données, les individus et maintenant « l'intelligence » sont désormais largement situés en dehors du périmètre physique des organisations. Au modèle de la confiance qui était accordée de façon implicite à chaque ressource dès lors qu'elle se situait en interne, succède donc un modèle où chaque équipement, chaque flux, chaque utilisateur, où qu'il soit, doit faire l'objet d'une vérification afin de s'assurer qu'il dispose bien des autorisations nécessaires.

Bref, un modèle de confiance explicite où aucune confiance n'est accordée par défaut sans vérification. Un modèle où la sécurité devient granulaire et multicouches. C'est le modèle *Zero Trust.*

Dans ce modèle, la confiance est donc institutionnalisée et systémique. Elle repose sur des processus, des normes, des contrats. Elle est conditionnelle, quantifiable, contextuelle, remplaçable et rationnelle. Elle est déléguée à des structures, des tiers de confiance. Elle s'appuie sur de multiples technologies, qu'il s'agisse d'authentification multi-facteurs, d'analyse comportementale, de chiffrement, de micro-segmentation. Certaines technologies, comme le Web3, permettent même - en théorie - d'automatiser la confiance grâce à des registres immuables réduisant encore la nécessité d'une confiance humaine directe, au prix cependant d'une transparence accrue, qui peut être source de contraintes, voire être attentatoire à nos libertés fondamentales. L'automatisation et la standardisation de la confiance, inhérente au monde relationnel, induisent par ailleurs un risque de dépersonnalisation, voire d'un transfert de responsabilité vers les systèmes, avec pour conséquence un risque d'une déresponsabilisation des individus et des organisations auquel il faut prendre garde.

L'adoption croissante du modèle *Zero Trust* n'est donc pas anodine. C'est une tendance sociétale, puis un modèle d'organisation avant d'être un projet technologique. Et c'est un projet d'entreprise, pas uniquement celui de la DSI ou du RSSI. C'est tout le mérite du travail mené par le groupe de travail *Zero Trust* mis en place par le Forum INCYBER, en partenariat avec le CESIN, et sous l'égide d'Eric Singer, que de démystifier ce concept et de faire le point sur son adoption au sein des entreprises.

Guillaume TISSIER

Directeur général du Forum INCYBER - Europe

IN CYBER
FORUM
EUROPE

INTRODUCTION

Pour la 17e édition du Forum INCYBER 2025, le thème retenu est « Au-delà du *Zero Trust*, la confiance pour tous ». Ce choix illustre l'évolution des stratégies de cybersécurité vers une approche qui ne se limite plus à la défiance systématique, mais cherche à rétablir un équilibre entre sécurité et confiance dans les écosystèmes numériques.

Représentant la communauté cybersécurité francophone, le CESIN s'associe au Forum INCYBER pour la réalisation de ce livre blanc : « *Zero Trust*, le nouveau paradigme ». Cette initiative a pour objectif de fournir une réflexion approfondie et opérationnelle sur la mise en œuvre du *Zero Trust* au sein des organisations, en s'appuyant sur les retours d'expérience concrets des membres du CESIN.

Un sondage réalisé auprès des membres du CESIN a réuni près de 200 réponses, mettant en lumière les enjeux, difficultés et succès rencontrés par les entreprises dans leur cheminement vers une architecture *Zero Trust*. En complément de cette étude, une dizaine de membres, désignés comme ambassadeurs de cette première initiative, ont activement participé à l'élaboration de ce livre blanc. Leur expertise et leur vision unique ont été essentielles pour enrichir cette analyse et apporter des perspectives variées sur ce sujet complexe.

Je tiens à exprimer toute ma gratitude à ces contributeurs engagés :

- Laurent BEAUPUIS (Klesia)
- Alain BOUILLÉ (CESIN)
- Fabrice BRU (CESIN)
- Guillaume CONTAT (Assemblée Nationale)
- Michel DUBOIS (La Poste)
- Cyril HAZIZA (Kering)
- Philippe LATOMBE (Assemblée Nationale)
- Vincent LEFRET (CESIN)
- Jean-François LOUAPRE (Agrial)
- Stéphane TOURNADRE (Servier)
- Frank VAN CAENEGEM (Schneider Electric / CESIN)
- Cyril VOISIN (Microsoft)

Ce livre blanc est structuré en plusieurs chapitres correspondant aux étapes clés de la mise en place d'une stratégie *Zero Trust* au sein d'une organisation. Il aborde successivement la compréhension du concept, son explication aux dirigeants, l'analyse des succès et des défis rencontrés, les aspects technologiques ainsi que des retours d'expérience concrets.

Pensé pour être un outil accessible et pragmatique, ce livre peut être lu de manière linéaire ou abordé directement par le prisme d'un chapitre spécifique. Que vous souhaitiez explorer la gestion des tiers dans une démarche *Zero Trust* ou comprendre pourquoi et comment adopter cette approche, vous trouverez ici des clés essentielles pour guider votre réflexion et vos actions.

Je vous souhaite une excellente lecture et espère que ce livre blanc saura vous fournir les éléments nécessaires pour mener à bien votre transformation vers un modèle *Zero Trust*.

Eric SINGER
Responsable du Cursus Cybersécurité
ESIEE-IT

Le concept du *Zero Trust*, longtemps considéré comme un *buzzword,* a fait, petit à petit, son chemin dans les approches cybersécurité des entreprises. Le CESIN mesure cette tendance depuis plusieurs années au travers de son Baromètre et on peut dire maintenant que cette approche est devenue quasiment incontournable dans toute démarche cybersécurité mature. Même si l'appellation *Zero Trust* n'est pas des plus heureuses pour marketer la cybersécurité, force est de constater que cette approche est très bénéfique pour la cyberdéfense.

Le Forum INCYBER a décidé d'en faire le thème central pour son édition 2025 et le CESIN est très heureux de vous proposer ce Livre Blanc sur cette thématique qui nous l'espérons, vous permettra d'appréhender ce concept avec plus de sérénité.

Fabrice BRU
Président
CESIN

Alain BOUILLÉ
Délégué général
CESIN

Pour vous présenter notre ouvrage de façon décalée et originale, j'ai commencé par demander à une IA générative de définir le concept *Zero Trust* dans le style de Victor Hugo... Voici le résultat :

PRÉSENTATION DU CONCEPT *ZERO TRUST* PAR UNE IA GÉNÉRATIVE DANS LE STYLE DE VICTOR HUGO

Dans l'ombre des réseaux où le danger s'insinue,
Un bastion se dresse, fort, contre l'inconnu.
C'est le Zero Trust, sentinelle éternelle,
Qui veille sans relâche, implacable et fidèle.

Nul accès n'est donné sans preuve et vérité,
Car la confiance aveugle engendre l'impiété.
Même l'ami d'hier, pour franchir le seuil clos,
Doit prouver son chemin, éviter les fardeaux.

Chaque requête inspecte, et chaque clé se lie,
À l'authentique trace de l'identité.
Point de privilège acquis, point de passe-droit,
Le doute est souverain, il forge notre loi.

Ainsi, dans ce rempart qu'aucun vent ne dérobe,
Le malheur se brise, et la menace s'robe.
Car dans ce monde vaste, obscur et dangereux,
Zero Trust est lumière, éclatant, vigoureux.

Ô fils du numérique, apprends cette vertu :
Ne fais foi qu'à la preuve, et nullement au vu.
C'est là la voie sacrée, la clé de l'avenir,
Pour que tes données vivent sans jamais périr.

QU'EST-CE QUE LE *ZERO TRUST* ?

BUZZWORD,

DÉMARCHE VERTUEUSE OU MARCHE DIFFICILE ?

*ZERO TRUST : U*N CHANGEMENT DE PARADIGME POUR LA CYBERSÉCURITÉ

Le concept de *Zero Trust* repose sur un principe fondamental : ne jamais accorder de confiance implicite, mais toujours vérifier explicitement. Défini par le NIST *(National Institute of Standards and Technology),* le *Zero Trust* étend le modèle traditionnel de sécurité périmétrique vers une approche plus granulaire de l'authentification et de l'autorisation, toujours dans l'idée de la défense en profondeur. Cependant, certains considèrent que l'appellation *Zero Trust* est un faux ami et qu'il serait plus approprié de parler de *Explicit Trust,* soulignant ainsi la nécessité d'un contrôle systématique des accès.

UNE DÉMARCHE VERTUEUSE ET PROGRESSIVE

Le *Zero Trust* ne constitue pas une rupture brutale mais plutôt une évolution vers une gouvernance renforcée des actifs numériques. Il permet d'améliorer le niveau de sécurité des organisations tout en s'adaptant aux nouvelles réalités des systèmes d'information dépérimétrés.

En adoptant cette approche, les organisations peuvent progressivement améliorer leur maturité en cybersécurité et répondre aux nouvelles menaces, en renforçant les contrôles et la gestion des accès, en optimisant et adaptant les mécanismes de détection et de surveillance.

ZERO TRUST EN ACTION : GOUVERNANCE ET IMPLÉMENTATION

Dans certaines organisations, le *Zero Trust* est partiellement en production et apporte une gouvernance précise des actifs informatiques. Il permet notamment une catégorisation par niveau de risque, une meilleure maîtrise des accès et une lutte contre le *Shadow IT* (utilisation de systèmes numériques sans l'approbation ou le contrôle de la direction des systèmes d'information de l'organisation).

Un projet *Zero Trust* réussi repose sur la confiance dans l'usage des systèmes d'information de l'organisation et à partir des aspects suivants :

— **Une identification et classification des ressources** qui permet d'inventorier les actifs à protéger et évaluer les risques encourus.

— **L'authentification renforcée et l'autorisation de chaque accès,** pouvant prendre en compte divers paramètres comme le lieu d'accès ou la confiance dans l'équipement utilisé par exemple.

— **La micro-segmentation réseaux et restriction des accès** qui permet de cloisonner différentes zones du réseau, limitant ainsi les mouvements latéraux.

— **La surveillance et analyse en temps réels des usages** qui permet de détecter des anomalies et des comportements suspects.

— **L'orchestration de la sécurité** qui facilite l'automatisation des politiques du *Zero Trust* et soulage les équipes de réponses à incidents de tâches répétitives et sans valeurs

— **Le principe du moindre privilège** qui permet de limiter des droits d'accès aux seuls besoins nécessaires.

— **La protection des données** par le biais de mécanismes de chiffrement et par l'utilisation de politiques de gestion adaptées.

Toutefois, la mise en œuvre du *Zero Trust* n'est pas sans défis. L'approche implique une transformation profonde de l'infrastructure, avec un déploiement progressif pour éviter les erreurs de configuration et garantir un contrôle fin des accès. Dans la pratique, elle se traduit souvent par un renforcement des processus de gestion d'identité, la micro-segmentation, et l'intégration de mécanismes de contrôle continu.

ENTRE PRAGMATISME ET *BUZZWORD*

Si certains CISOs perçoivent le *Zero Trust* comme une philosophie de protection explicite permettant de sécuriser les nouveaux usages comme le « BYOD » *(Bring Your Own Device),* en français « AVPA » (Apportez Votre Propre Appareil), le nomadisme ou le *Move to Cloud,* d'autres y voient un simple buzz marketing exploité par les fournisseurs.

Une approche *Zero Trust* peut être mise en œuvre en fonction du contexte de l'organisation et du niveau de maturité en cybersécurité existant. Le *Zero Trust* est une approche sur-mesure et il est utile de questionner les solutions proposées par certains éditeurs, qui se disent *Zero Trust*, sans pour autant prendre en compte le contexte et besoin de l'organisation.

Le *Zero Trust* est une approche globale qui revisite la posture de sécurité des organisations de manière holistique, prenant en compte la gestion des accès et la protection des actifs numériques par exemple. Les organisations qui s'engagent dans cette démarche doivent anticiper les coûts et les difficultés techniques, mais les bénéfices en termes de sécurité et de résilience en valent la peine. Son implémentation peut paraître complexe, mais elle répond à l'évolution des menaces et à la nécessité de contrôler chaque accès avec une granularité accrue. Le *Zero Trust* représente ainsi une transformation stratégique nécessaire pour faire face à un environnement de menaces en perpétuelle évolution.

CE QU'IL FAUT RETENIR

Le *Zero Trust* est une stratégie de sécurité holistique exigeant une vérification continue et rigoureuse de chaque demande d'accès, tout en minimisant les privilèges et en segmentant le réseau pour réduire les risques.

Contrairement à la sécurité périmétrique traditionnelle, cette philosophie explicite pourrait permettre de relever les défis actuels de la cybersécurité. Elle représente une évolution des modèles de cybersécurité, tenant compte de la dépérimétrisation des systèmes d'information, et permet d'améliorer et d'accroître le niveau de maturité en matière de sécurité au sein d'une organisation.

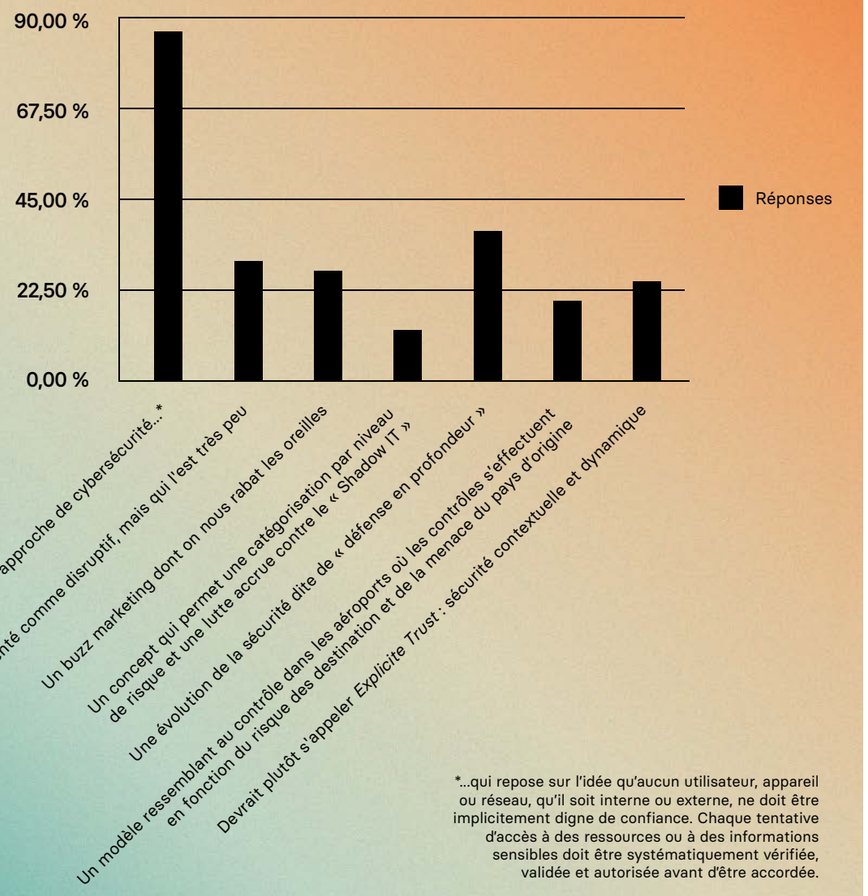
« Le concept de *Zero Trust* apporte une gouvernance des actifs. Il permet une catégorisation par niveau de risque et une lutte accrue contre le *Shadow IT.* »

Stéphane TOURNADE
Servier

« Le *Zero Trust* est une philosophie prônant une sécurité explicite, par opposition à la sécurité périmétrique traditionnelle. »

Cyril VOISIN
Microsoft

POUR VOUS LE CONCEPT DE *ZERO TRUST* EST...



*...qui repose sur l'idée qu'aucun utilisateur, appareil ou réseau, qu'il soit interne ou externe, ne doit être implicitement digne de confiance. Chaque tentative d'accès à des ressources ou à des informations sensibles doit être systématiquement vérifiée, validée et autorisée avant d'être accordée.

2 PARLER *ZERO TRUST* AU COMEX

CONTEXTUAL TRUST : UNE AUTRE MANIÈRE DE PARLER DU *ZERO TRUST*

Dans la situation actuelle de transformation digitale, il est nécessaire d'adopter une stratégie de sécurité adaptée aux risques de l'organisation. Le *Zero Trust*, pouvant aussi s'appeler *Contextual Trust,* repose sur la vérification systématique de chaque demande d'accès, en tenant compte du contexte et du niveau de risque associé. Par défaut, aucun utilisateur, appareil ou réseau – qu'il soit interne ou externe – n'est considéré comme digne de confiance.

ORIGINE ET ÉVOLUTION DU CONCEPT

Formalisé en 2010 par John Kindervag, analyste chez Forrester, le modèle *Zero Trust* est une réponse aux limites du traditionnel « château fort » qui protégeait uniquement un périmètre établi. Aujourd'hui, avec l'essor du *Cloud*, du télétravail et de la mobilité, le périmètre de l'organisation est devenu flou. Le *Zero Trust* est avant tout une approche de sécurisation fine des accès et des interactions. Le terme *Contextual Trust,* pourrait paraître plus adapté que celui de *Zero Trust* ; l'objectif est de réduire les risques et de répondre aux besoins métiers afin de sécuriser les accès en fonction des menaces.

Quelques exemples :

— **Authentification adaptative :** Dans le secteur bancaire, l'authentification multi-facteurs est utilisée pour valider chaque transaction. Lorsqu'un utilisateur se connecte depuis un nouvel appareil ou dans un contexte inhabituel, des contrôles supplémentaires sont déclenchés pour vérifier son identité.

— **Détection des comportements anormaux :** Les systèmes de surveillance analysent en temps réel les comportements d'accès. Par exemple, si un utilisateur tente d'accéder à des données sensibles en dehors des heures habituelles, des vérifications additionnelles sont automatiquement mises en place afin d'éviter toute compromission.

— **Protection contre les menaces émergente :** Face à des attaques sophistiquées, telles que celles exploitant l'intelligence artificielle, la sécurité dépérimétrée permet d'identifier rapidement les anomalies et de réagir en conséquence, en concentrant les moyens de protection sur les risques les plus critiques.

CRÉATION DE VALEUR ET RETOUR SUR INVESTISSEMENT

Le *Zero Trust* basé sur les risques, optimise l'allocation des ressources et oriente les investissements vers les mesures prioritaires à fort impact. Cette démarche permet de :

— **Réduire le nombre d'incidents de sécurité**, ce qui se traduit par une diminution des coûts liés aux interruptions de service et aux corrections d'incidents.

— **Renforcer la confiance des clients et partenaires**, en assurant une disponibilité de service et une protection accrue des données sensibles.

— **Améliorer la visibilité et la maitrise sur l'ensemble des accès**, facilitant ainsi la gestion proactive des risques.

CE QU'IL FAUT RETENIR :

Adopter le *Zero Trust*, c'est investir dans une stratégie évolutive et performante, adaptée aux défis actuels et futurs du paysage numérique de l'organisation.

Pour assurer la réussite de cette transformation, le soutien du COMEX est indispensable, permettant d'impulser une gestion du changement, garantissant une harmonisation des initiatives de cybersécurité et renforçant la résilience globale de l'organisation.

« Le lien du *Zero Trust* avec la stratégie cyber réside dans le travail en amont qui doit être réalisé pour définir les orientations organisationnelles et techniques à décider. »

Guilaume CONTAT
Assemblée Nationale

« Le *Zero Trust* doit être compréhensible par le Comex pour avoir son support, et peut facilement être expliquer comme l'évolution des contrôles aéroportuaires en fonction des risques actualisés et des évolutions technologiques. »

Frank VAN CAENEGEM
Schneider Electric / CESIN

3 POURQUOI ADOPTER UNE DÉMARCHE ZERO TRUST ?

LE *ZERO TRUST :* MOTIVATIONS ET DÉFIS POUR UNE ADOPTION EN ORGANISATION

Depuis plusieurs années, l'évolution des menaces et des usages informatiques pousse les organisations à revoir leurs modèles de sécurité. Traditionnellement fondé sur une approche périmétrique, le modèle « château fort » a montré ses limites face à l'adoption massive du *Cloud*, à la mobilité et au recours au BYOD *(« Bring Your Own Device »)*.

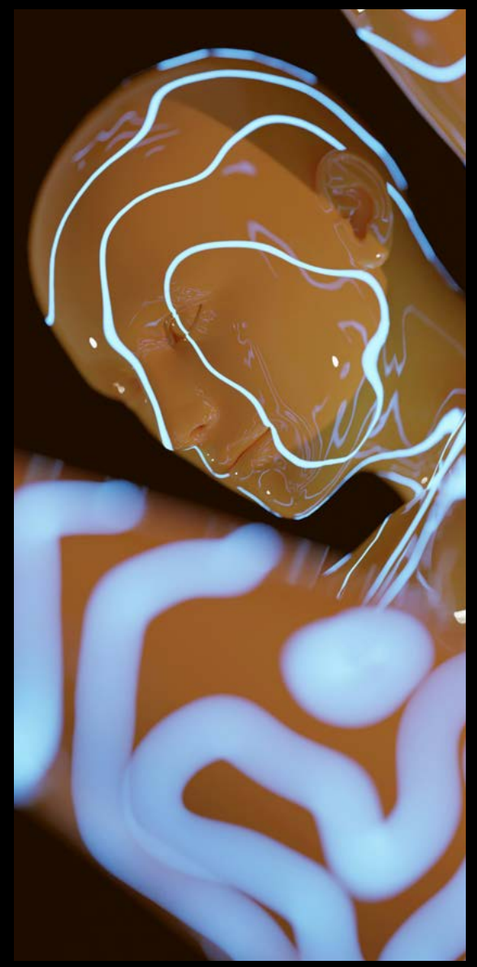
Dans ce contexte, le concept de *Zero Trust* suscite un intérêt croissant. Plutôt qu'un simple changement technologique, il s'agit d'une philosophie visant à renforcer la cybersécurité par une approche fondée sur la vérification systématique des accès et des identités.

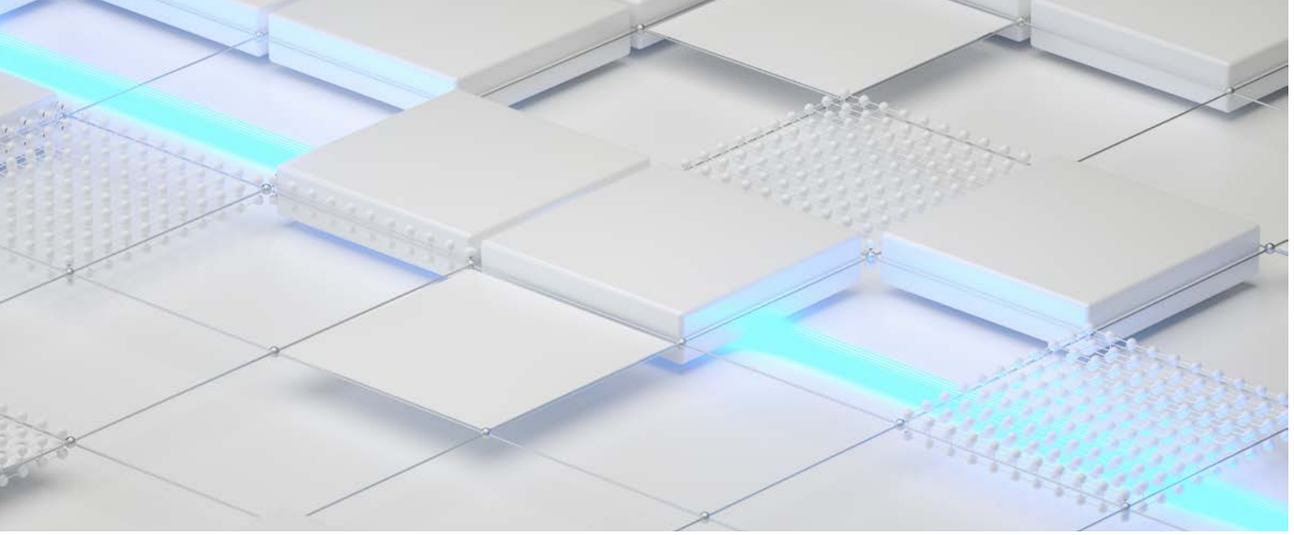
Toutefois, l'adoption d'une telle approche ne va pas de soi. Elle implique une transformation en profondeur des architectures informatiques et soulève des enjeux organisationnels, techniques, métiers et culturels. De nombreuses organisations, conscientes de ces défis, s'interrogent sur les meilleures manières d'aborder ce virage et d'en mesurer les bénéfices.

UNE ÉVOLUTION NÉCESSAIRE, MAIS PAS RÉVOLUTIONNAIRE

Un constat s'impose souvent : « Nous faisons déjà du *Zero Trust*, souvent sans le savoir ». En effet, plusieurs principes sous-jacents à ce modèle sont déjà appliqués dans les politiques de sécurité des organisations : authentification multi-facteur (MFA), segmentation réseau, accès conditionnels basés sur le contexte. L'adoption du *Zero Trust* ne constitue donc pas une rupture brutale mais plutôt une évolution vers une approche plus structurée et systématique.

L'un des apports majeurs de ce modèle est sa capacité à contextualiser les accès en fonction de divers paramètres : identité de l'utilisateur, appareil utilisé, localisation, comportement inhabituel. Ce niveau de granularité supplémente les mécanismes traditionnels et réduit les risques d'attaques par usurpation d'identité ou de mouvements latéraux dans le système d'information.





QUELLE EST LA MÉTHODE ET QUELS SONT LES DÉFIS D'UNE TELLE APPROCHE ?

Dans le modèle *Zero Trust*, la demande d'accès, par un utilisateur, à une ressource de l'organisation est accordée via un Point de Décision de Politique (PDP) et un Point d'Application de Politique (PEP) correspondant. Le système doit alors garantir que l'utilisateur est authentique et que la demande est valide. Le PDP/PEP prend une décision appropriée pour autoriser le sujet à accéder à la ressource. Cela signifie que le *Zero Trust* s'applique à deux domaines de base : l'authentification et l'autorisation. Cela implique également que la mise en œuvre de manière holistique du *Zero Trust* nécessite de relever les défis suivants :

1. **Complexité d'intégration et de transformation**

   Le passage à une architecture *Zero Trust* implique une revue des systèmes existants, notamment en matière de réseau, de gestion des identités et d'administration des accès. Les organisations doivent définir des stratégies claires de segmentation et de gestion fine des autorisations. Cette transformation peut s'avérer longue et coûteuse, en particulier pour les structures aux systèmes hérités complexes.

2. **Gestion des identités et des accès (IAM)**

   L'un des pivots du *Zero Trust* repose sur une identification et une authentification rigoureuse des utilisateurs et de leurs dispositifs digitaux. Les organisations doivent s'appuyer sur des solutions modernes et robustes de gestion des identités et des accès, tout en s'assurant que ces mécanismes ne nuisent pas à l'expérience utilisateur.

3. **Surveillance et réaction en temps réel**

   Une approche *Zero Trust* efficace requiert une supervision constante des activités sur les réseaux informatiques et une capacité à détecter et à réagir rapidement aux anomalies. Cette vigilance impose une augmentation du volume de données à analyser, ce qui peut poser des problèmes de passage à l'échelle et de charge opérationnelle pour les équipes de cybersécurité.

4. **Adoption interne et gestion du changement**

   L'implémentation du *Zero Trust* peut rencontrer des résistances en interne, notamment au sein des équipes informatiques et des utilisateurs finaux. Le sentiment d'un système plus contrôlant et contraignant peut nuire à l'adhésion des collaborateurs si les bénéfices ne sont pas clairement expliqués et si les changements ne sont pas accompagnés par des formations adaptées.

UN LEVIER POUR LA STRATÉGIE CYBER ET LA CONFORMITÉ

Malgré ces difficultés, le *Zero Trust* trouve une résonance forte dans la stratégie cyber des organisations. L'approche permet de :

— **Réduire la surface d'attaque** en limitant les accès aux seules ressources nécessaires.

— **Renforcer la résilience** face aux cyberattaques grâce à un contrôle continu et granulaire.

— **Améliorer la conformité réglementaire,** notamment avec les exigences du RGPD, de la directive NIS2 ou des standards comme SecNumCloud.

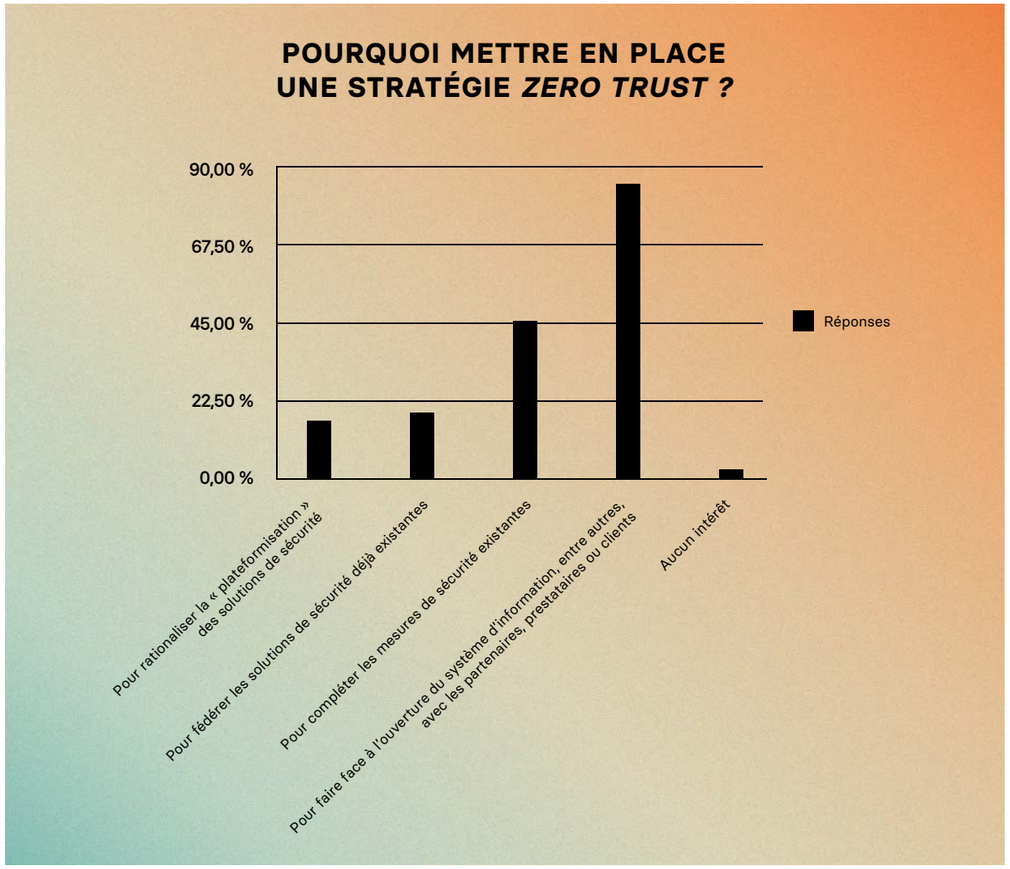
— **Accélérer la détection et la réponse aux incidents** via une surveillance plus fine et adaptée au contexte des accès.

CE QU'IL FAUT RETENIR

Adopter une approche *Zero Trust* peut permettre de répondre aux évolutions des menaces et des usages numériques. Cependant, cette transformation ne se fait pas sans difficultés et doit être abordée de manière progressive et pragmatique. Plutôt qu'un objectif à atteindre de manière absolue, le *Zero Trust* peut être vu comme un cadre permettant d'améliorer en continu la posture de sécurité des organisations. Son implémentation doit être guidée par une vision claire, une coordination forte entre les différentes parties prenantes et un équilibre entre sécurité et expérience utilisateur.

« Le *Zero Trust* vient en complément des fondamentaux cybersécurité quand ceux-ci sont en place et maitrisés. »

Jean-François LOUAPRE
Agrial



4 QUELS SONT LES PRINCIPAUX ÉLÉMENTS CLÉS POUR UN PROJET *ZERO TRUST* RÉUSSI ?

LE *ZERO TRUST* EN CYBERSÉCURITÉ : CLÉS DE SUCCÈS ET POINTS D'ATTENTION

La mise en œuvre d'une stratégie *Zero Trust* réussie est un projet d'envergure qui requiert une approche rigoureuse et coordonnée.

PRINCIPES CLÉS DU *ZERO TRUST*

Une architecture *Zero Trust* repose sur les principes suivants :

1. **Toutes les données et services informatiques sont considérés comme des ressources.**

   Le réseau informatique englobe divers types d'appareils, y compris ceux à faible encombrement (IoT, actionneurs), des solutions Cloud/SaaS et des systèmes d'agrégation de données. Une organisation peut également considérer les appareils personnels comme des ressources s'ils accèdent aux systèmes de l'organisation.

2. **Toutes les communications sont sécurisées, indépendamment de leur emplacement.**

   L'accès aux ressources ne doit pas être basé sur la position du réseau, mais sur des contrôles de sécurité cohérents. Les connexions internes et externes sont soumises aux mêmes exigences de sécurité afin d'assurer confidentialité, intégrité et authentification.

3. **L'accès aux ressources est accordé de manière dynamique et limitée à chaque session.**

   L'autorisation d'accès repose sur une évaluation continue du niveau de confiance, appliquant les principes du moindre privilège. Une authentification préalable à une ressource ne garantit pas l'accès aux autres.

4. **Les décisions d'accès sont basées sur une politique dynamique et contextuelle.**

   L'accès est déterminé par l'identité du demandeur (utilisateur, service, application), l'état de l'appareil (version logicielle, emplacement, comportement) et des facteurs environnementaux (menaces en cours, fuseau horaire, wifi public, etc.). Ces politiques d'autorisation évoluent selon la sensibilité des ressources.

5. **L'intégrité et la sécurité des actifs sont surveillées en continu.**

   Aucun appareil n'est intrinsèquement fiable. L'organisation doit détecter les vulnérabilités, appliquer les correctifs et évaluer la conformité des actifs avant d'accorder un accès. Les appareils compromis ou non gérés peuvent être restreints ou bloqués.

6. **L'authentification et l'autorisation sont dynamiques et systématiquement appliquées.**

   L'accès est soumis à une validation constante, intégrant l'authentification multifacteur (MFA) et des mécanismes de surveillance. Une réévaluation de la confiance intervient en fonction des changements de contexte (nouvelle requête, comportement suspect, voyage impossible, etc.), garantissant un équilibre entre sécurité et expérience utilisateur.

7. **Les données de sécurité sont collectées et exploitées en continu.**

   L'organisation doit analyser l'état des actifs, le trafic réseau et les demandes d'accès pour affiner ses politiques de sécurité et améliorer sa posture globale.

CLÉS DU SUCCÈS D'UN PROJET *ZERO TRUST*

1. ***Sponsorship* global et gouvernance adaptée**

   L'adoption du *Zero Trust* est une initiative transverse qui impacte différents métiers de l'organisation. Il est essentiel d'obtenir un soutien au plus haut niveau, notamment auprès du COMEX. Le RSSI/CISO joue ici un rôle de chef d'orchestre, assurant la coordination entre la DSI, les directions digitales et métiers et les opérations de cybersécurité.

2. **Une maturité suffisante en gestion des risques et des identités**

   Avant d'entamer un projet *Zero Trust*, une cartographie précise des risques et des actifs est nécessaire. Une gestion robuste des identités, des profils et des accès constitue également un prérequis fondamental pour garantir une mise en œuvre fluide.

3. **Une approche progressive et contextualisée**

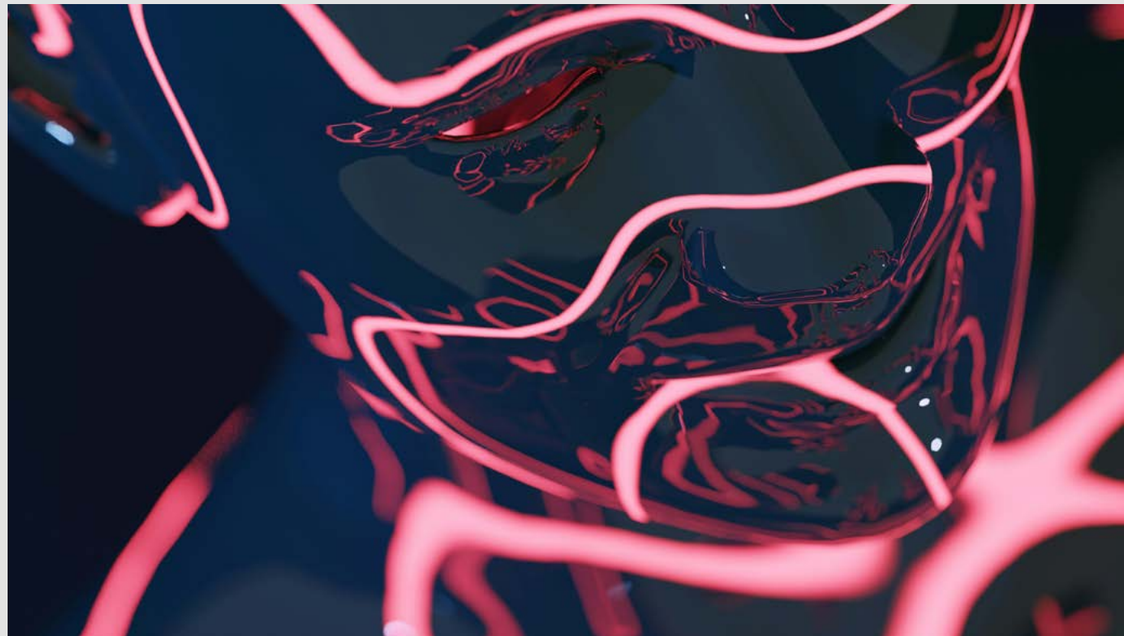
   Plutôt qu'un basculement radical, une approche progressive, par priorisation des systèmes critiques et des flux sensibles, permet une transition mieux contrôlée.

4. **Une intégration fluide et transparente**

   Le succès d'un projet *Zero Trust* repose sur l'absence de friction pour les utilisateurs. Les politiques de sécurité doivent être calibrées pour garantir un niveau de protection maximal tout en assurant une expérience utilisateur fluide.

5. **La conduite du changement**

   La mise en place d'un *Zero Trust* efficace nécessite un accompagnement des collaborateurs. Sensibilisation, formation et adaptation des processus organisationnels sont des éléments incontournables.



MODÈLES D'ANALYSE ET STRATÉGIES DE MISE EN ŒUVRE

1. **L'*Airline Model of Zero Trust***

   Inspiré de la sécurité aérienne, ce modèle repose sur une surveillance continue et une évaluation dynamique des risques. Chaque accès est traité comme un passage à un poste de contrôle, avec des vérifications systématiques.

2. **Matrice de risque à cinq entrées**

   Un cadre d'évaluation des risques reposant sur cinq critères : identité, appareil, localisation, comportement et sensibilité de la ressource demandée. Cet outil permet de déterminer les conditions d'accès et d'adapter la politique de contrôle en conséquence.

3. **Zoning et micro-segmentation**

   L'organisation du SI en zones cloisonnées permet de limiter la propagation des menaces et de restreindre les accès à un périmètre précis. Cette segmentation fine est essentielle pour garantir l'efficacité du *Zero Trust*.

POINTS D'ATTENTION

1. **Prise en compte des impacts organisationnels et budgétaires**

   L'implémentation d'un cadre *Zero Trust* demande des ressources importantes, tant en termes humains que financiers. Il est crucial d'obtenir une adhésion de la direction en justifiant les investissements nécessaires.

2. **Difficulté d'application aux environnements hétérogènes**

   Un système d'information trop complexe, contenant de nombreux actifs historiques dit *legacy*, complique la mise en place du *Zero Trust*. Une rationalisation préalable est souvent requise.

3. **Adoption par les administrateurs systèmes et réseaux**

   Les comptes d'administration, comptes techniques, comptes partenaires…représentent un enjeu critique. Ils doivent être soumis à des règles encore plus strictes, ce qui peut se heurter à des r ésistances de la part des intéressés.

4. **Risques d'entrave à la productivité**

   Un excès de contrôles peut nuire à l'efficacité opérationnelle. Il est essentiel de calibrer les paramètres de sécurité en fonction des risques réels et des besoins métier. L'automatisation est également un levier à considérer.

5. **Protection des données à caractère personnel**

   La forte augmentation de la collecte de données (géolocalisation des terminaux, horaires, BYOD…), nécessaire à la quantification des risques en temps réel, soulèvent des questions légitimes en matière de protection des données. L'information des collaborateurs et des partenaires, la collaboration avec les délégués à la protection des données et le suivi des recommandations des autorités (CNIL, ANSSI…) apportent les garanties adaptées à cet enjeu essentiel.

INDICATEURS DE SUCCÈS

- Réduction de la gravité des incidents de sécurité
- Amélioration de la résilience informatique
- Respect des conformités réglementaires
- Adoption et satisfaction des utilisateurs
- Réduction du shadow IT

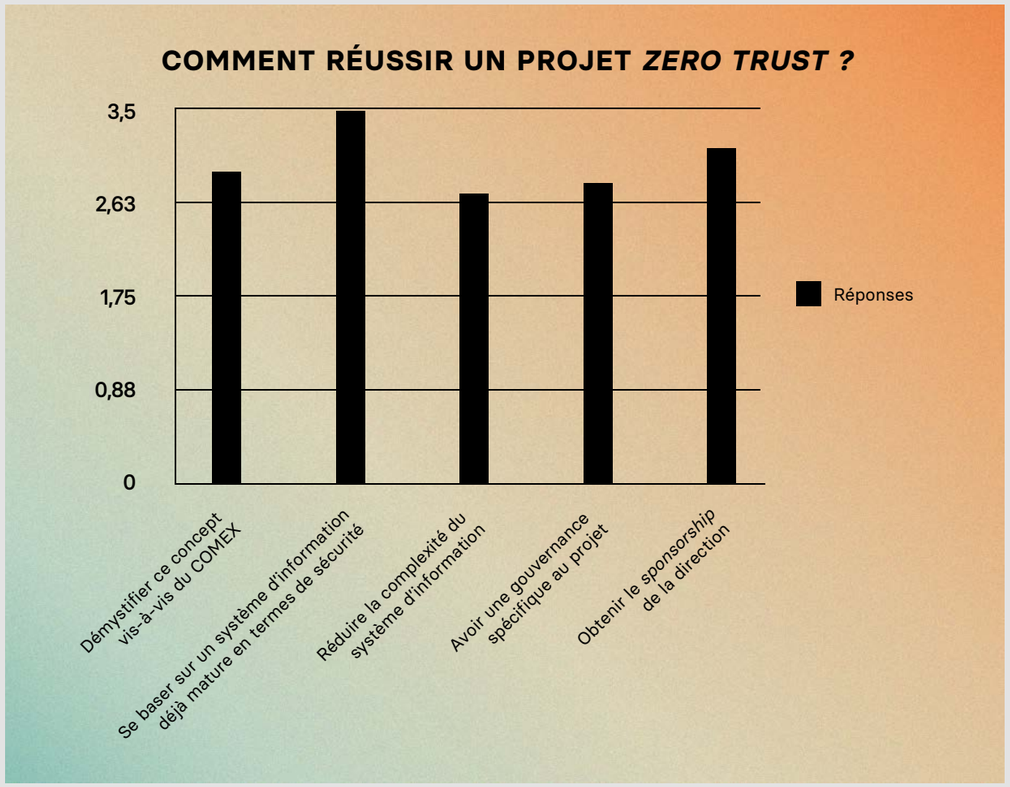
CE QU'IL FAUT RETENIR

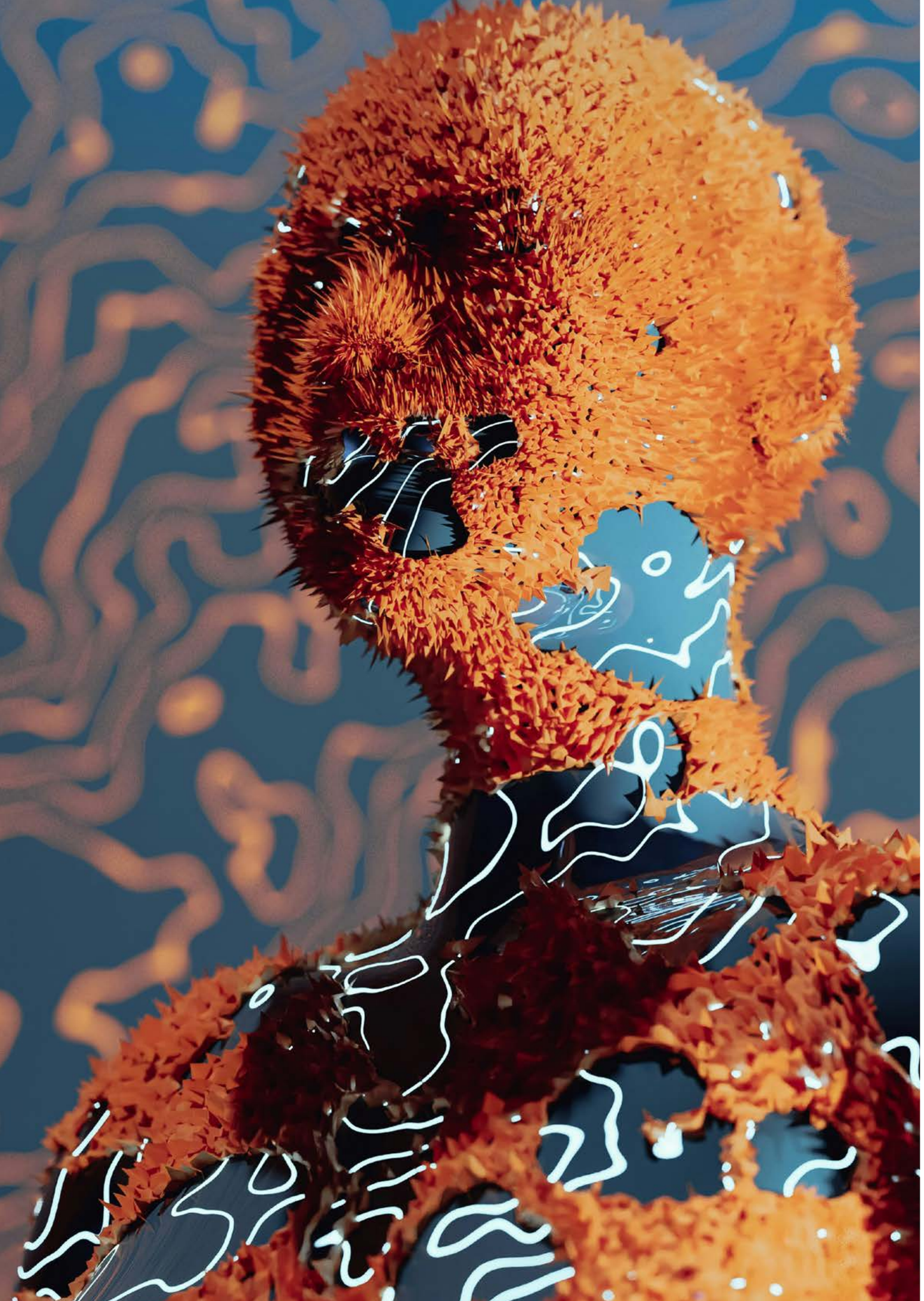
En synthèse, *Zero Trust* est un changement de paradigme qui redéfinit la manière dont les organisations protègent leurs ressources et accès. Son implémentation réussie repose sur une approche progressive, une gouvernance solide et une conduite du changement adaptée.

Une stratégie *Zero Trust* bien exécutée se traduit par une sécurité renforcée afin de lutter plus efficacement contre les fraudes et tentatives d'attaques tout en assurant un accompagnement des utilisateurs pour une meilleure expérience des outils sécurité.

« Le succès d'un projet *Zero Trust* se caractérise par une réduction significative des risques de sécurité, une gestion proactive des accès, une détection rapide des menaces et une expérience utilisateur. »

Cyril HAZIZA
Kering





5 QUEL EST L'ÉTAT ACTUEL DE L'ADOPTION DU *ZERO TRUST* ?

L'ÉTAT ACTUEL D'ADOPTION DU *ZERO TRUST :* ENTRE AVANCÉES ET RÉALITÉS DU TERRAIN

Le *Zero Trust* s'impose progressivement comme un modèle de référence en cybersécurité, mais son adoption varie considérablement d'une organisation à l'autre. Loin d'être un cadre unique et universel, il se décline sous différentes approches, adaptées aux contraintes et priorités de chaque organisation. Si certaines ont amorcé une transformation profonde en ce sens, d'autres peinent à l'envisager à court terme en raison de leurs systèmes existants et de leurs priorités opérationnelles.

UNE ADOPTION PROGRESSIVE ET CONTEXTUELLE

Il est important de souligner que l'adoption du *Zero Trust* ne signifie pas nécessairement un basculement complet et immédiat. De nombreuses organisations ont mis en place des éléments de *Zero Trust* sans forcément les désigner comme tels. L'authentification multifacteur (MFA), la micro-segmentation, l'extension du principe de moindre privilège ou encore l'observabilité accrue des infrastructures sont autant de pratiques qui s'inscrivent dans cette logique. En ce sens, le *Zero Trust* apporte une cohérence aux initiatives déjà en place, plutôt qu'une refonte complète et systématique.

Certaines organisations ont adopté une approche progressive en ciblant des périmètres spécifiques. Il est fréquent de commencer par sécuriser l'accès des utilisateurs avant d'élargir le modèle aux applications et aux ressources critiques. Cela permet d'obtenir des gains rapides et d'engager une dynamique qui pourra s'étendre au fil du temps.

LES DÉFIS D'UNE IMPLÉMENTATION À GRANDE ÉCHELLE

Si le modèle *Zero Trust* s'appuie sur des principes clairs – accès conditionnel, surveillance continue, politique de moindre privilège – sa mise en œuvre complète reste complexe. Plusieurs freins sont régulièrement cités :

— **Le poids du *legacy* :** Certains systèmes anciens ne permettent pas toujours d'appliquer des principes *Zero Trust* de manière fluide. Toutefois, cela n'empêche pas d'adopter une approche segmentée et d'introduire progressivement des mécanismes de sécurisation sur des périmètres maîtrisés.

— **La réticence des équipes IT et administrateurs** : Le changement de paradigme induit par le *Zero Trust*, qui remet en cause les modèles classiques de confiance implicite, peut être mal perçu. La mise en œuvre demande un accompagnement fort pour éviter des résistances internes.

— **Un terme parfois mal compris** : L'expression Z*ero Trust* peut être anxiogène et donner l'impression d'un manque de confiance généralisé, alors qu'il s'agit avant tout d'une sécurisation fine des accès et des interactions.

— **L'enrôlement des utilisateurs et des systèmes** : Si certains aspects du *Zero Trust* sont bien avancés (MFA, accès conditionnel), d'autres restent plus complexes à généraliser, notamment l'inventaire exhaustif des actifs et la gestion dynamique des identités et des tiers.

DES AVANCÉES SIGNIFICATIVES DANS LES ORGANISATIONS

Malgré ces défis, des organisations ont engagé des projets structurants à partir d'un projet *Zero Trust*. Voici quelques tendances observées :

- **Déploiement progressif des accès conditionnels :** plusieurs organisations ont formalisé une directive spécifique dans leur politique de sécurité des systèmes d'information (PSSI) pour encadrer les modalités d'Authentification et d'Autorisation.
- **Unification des systèmes d'IAM :** l'intégration de toutes les applications au sein d'une solution IAM centralisée est un chantier clé pour renforcer la gestion des identités et des accès.
- **Surveillance accrue et amélioration de la détection :** le SOC joue un rôle essentiel dans l'approche *Zero Trust*, avec une meilleure observabilité des flux et une consolidation des journaux d'événements via un SIEM.
- **Renforcement des infrastructures critiques :** des efforts sont menés pour améliorer la classification des données, la segmentation des réseaux et la mise en place de solutions comme le DLP (protection contre la fuite d'information) ou l'EDR (protection contre du contenu malveillant sur les postes de travail).
- **Expérience utilisateur et flexibilité des accès :** certaines organisations ont orienté leur stratégie *Zero Trust* vers une approche plus fluide et webisée, avec des agents ZTNA *(Zero Trust Network Access)* facilitant l'accès sécurisé aux ressources.

VERS UNE GÉNÉRALISATION DU MODÈLE ?

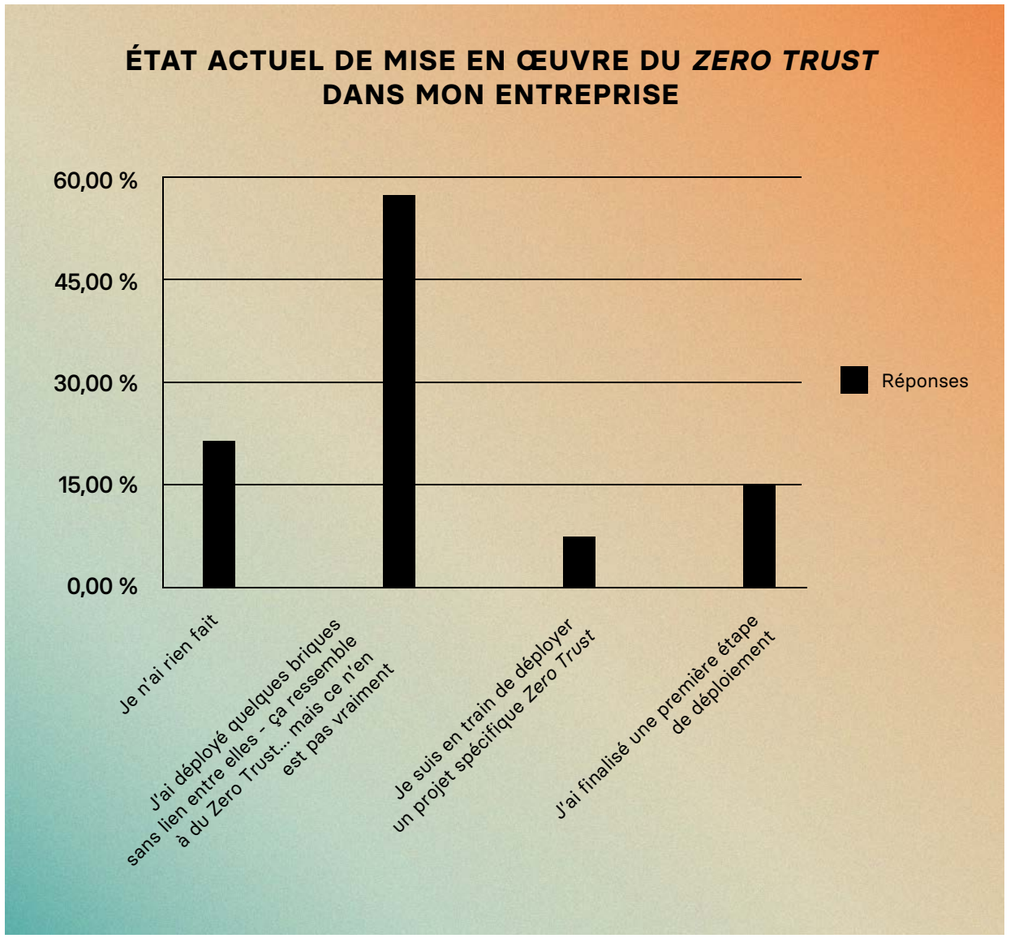
Si le *Zero Trust* a gagné du terrain et s'intègre progressivement dans les stratégies de cybersécurité, il reste du chemin à parcourir pour une mise en œuvre complète et homogène.

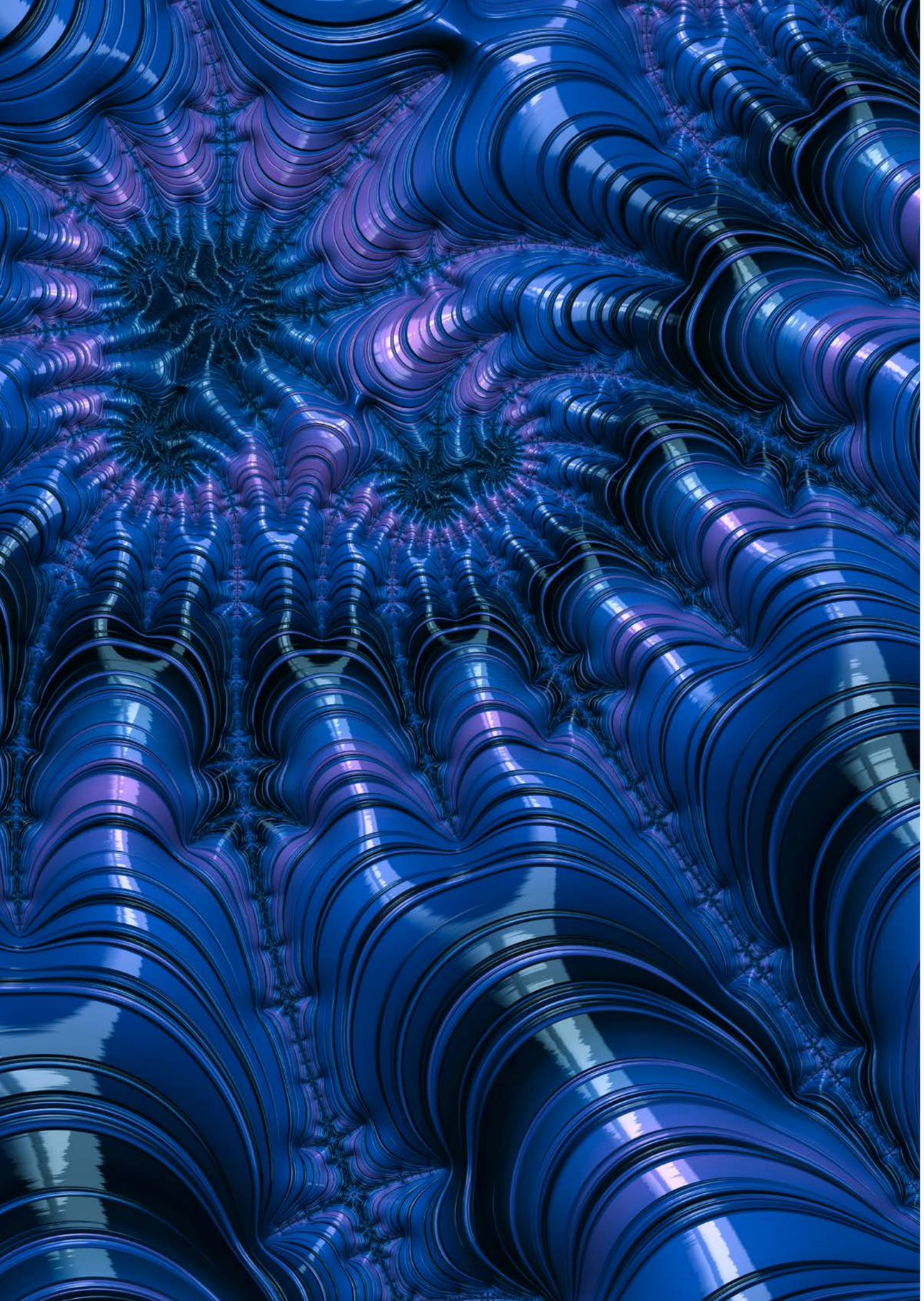
Certains environnements, notamment dans l'IT, ont déjà bien avancé, tandis que l'extension au monde OT ou aux infrastructures plus anciennes reste un sujet en cours d'exploration. De même, l'adoption du *Zero Trust* dépend des priorités des organisations : certaines privilégient encore des *quick wins* sur les fondamentaux de la cybersécurité avant d'engager une transformation plus large.

CE QU'IL FAUT RETENIR :

Le *Zero Trust* n'est pas une simple superposition d'outils, mais un modèle qui repose sur une gouvernance, des politiques claires et une surveillance continue. Son succès passe par une approche progressive et adaptée, qui tienne compte des réalités organisationnelles et techniques de chaque organisation.

ÉTAT ACTUEL DE MISE EN ŒUVRE DU *ZERO TRUST* DANS MON ENTREPRISE





6

QUELLE SONT LES SOLUTIONS OU TECHNOLOGIES POUR METTRE EN ŒUVRE UNE ARCHITECTURE

ZERO TRUST

EFFICACE ?

TECHNOLOGIES ET OUTILS DU *ZERO TRUST* : UN PAYSAGE EN ÉVOLUTION

L'approche *Zero Trust* ne repose pas sur une technologie unique, mais sur un ensemble de principes et de solutions complémentaires visant à sécuriser les accès et les communications dans les environnements numériques modernes. Contrairement à certaines idées reçues, il n'existe pas de palette unique d'outils dédiés au *Zero Trust*. Seule la brique *Zero Trust* Network Access peut être considérée comme une technologie propre au modèle *Zero Trust*, les autres éléments étant des composantes de cybersécurité préexistantes intégrées dans une approche plus globale.

Des solutions technologiques variées et interdépendantes

ZTNA : UNE BRIQUE INCONTOURNABLE

Le *Zero Trust* Network Access (ZTNA) est souvent perçu comme l'unique technologie véritablement associée au modèle *Zero Trust*. Son principe repose sur un contrôle strict des accès aux ressources en fonction du contexte, du profil de l'utilisateur et de l'état de son terminal. Il s'appuie sur des mécanismes de reverse proxy, de segmentation fine et d'authentification renforcée pour garantir un accès granulaire et dynamique aux applications et services.

Cependant, le ZTNA ne constitue pas une solution complète en soi : il s'inscrit dans un écosystème de sécurité plus large, où d'autres technologies viennent compléter son action.

LA GESTION DES IDENTITÉS ET DES ACCÈS (IAM)

L'authentification multi-facteur (MFA) et la gestion des accès conditionnels sont des éléments clés de l'approche *Zero Trust*. L'implémentation de standards tels que FIDO2 permet de renforcer la sécurité sans sacrifier l'expérience utilisateur.

La gestion des identités (IAM) permet également d'adopter des approches plus sophistiquées comme le *Behavior-Based Access Control* (BBAC), qui ajuste les permissions en fonction du comportement de l'utilisateur. De plus, un travail approfondi sur les référentiels d'identité et la gouvernance des accès est souvent nécessaire pour assurer la cohérence et l'efficacité des stratégies *Zero Trust*.

MICRO-SEGMENTATION : UNE APPROCHE RÉSEAU GRANULAIRE

L'un des piliers du *Zero Trust* consiste à limiter les mouvements latéraux en appliquant des principes de segmentation stricte au sein des environnements informatiques. La micro-segmentation permet d'isoler les ressources critiques et d'empêcher un attaquant de se déplacer librement en cas de compromission d'un point d'entrée.

Toutefois, sa mise en œuvre peut être complexe, notamment en raison du manque de visibilité sur les actifs et des difficultés d'inventaire. Une approche progressive, en commençant par des segments clairement identifiés (utilisateurs privilégiés, applications sensibles, accès Internet, etc.), est souvent préférable.

SURVEILLANCE ET ANALYSE DES *LOGS* : VERS UNE VUE UNIFIÉE

Le *Zero Trust* nécessite une surveillance continue des activités pour détecter toute anomalie et ajuster dynamiquement les contrôles d'accès. La collecte et la centralisation des logs issus des différentes solutions de sécurité sont essentielles pour obtenir une visibilité globale.

Certaines organisations mettent en place un puits de *logs* unique afin de corréler les événements provenant des outils IAM, ZTNA, EDR, SIEM, et autres. Cela favorise une meilleure orchestration et permet aux centres de sécurité opérationnelle (SOC) d'exploiter ces informations via des solutions SOAR *(Security Orchestration, Automation, and Response)* pour accélérer la réponse aux incidents.

SASE : UN CADRE POUR LES FÉDÉRER TOUS ?

Le terme SASE signifie *Secure Access Service Edge* (Périphérie de Service d'Accès Sécurisé). Il s'agit d'un cadre architectural défini par Gartner qui combine plusieurs technologies de sécurité et de réseau pour fournir une sécurité complète et cohérente aux utilisateurs, applications et données, où qu'ils se trouvent.

Le SASE intègre plusieurs fonctionnalités clés, notamment :

1. **SD-WAN *(Software-Defined Wide Area Network)* :** Pour optimiser et sécuriser les connexions réseau entre différents sites.
2. **FWaaS *(Firewall as a Service)* :** Pour fournir des capacités de pare-feu dans le *Cloud*.
3. **SWG *(Secure Web Gateway)* :** Pour filtrer et sécuriser le trafic web.
4. **CASB *(Cloud Access Security Broker)* :** Pour sécuriser l'accès aux applications *Cloud*.
5. **ZTNA *(Zero Trust Network Access)* :** Pour appliquer les principes de la sécurité *Zero Trust*, chaque accès est vérifié et authentifié.

L'objectif du SASE est de simplifier la gestion de la sécurité et du réseau en consolidant ces fonctionnalités dans une plateforme unique, généralement délivrée en tant que service *Cloud*. Cela permet aux entreprises de protéger leurs ressources de manière uniforme, que les utilisateurs soient sur site, à distance ou en déplacement.

Une approche pragmatique et progressive

DES MESURES QUI NE SONT PAS EXCLUSIVES AU *ZERO TRUST*

Si les outils mentionnés précédemment sont essentiels dans une démarche *Zero Trust*, ils ne sont pas nécessairement spécifiques à cette approche. Beaucoup d'organisations ont mis en place ces technologies indépendamment du *Zero Trust*, sans pour autant formaliser un programme *Zero Trust* à part entière.

Par exemple, l'adoption généralisée du MFA, l'essor des solutions de détection et réponse (XDR, EDR), ou encore le déploiement du DLP pour la protection des données sont autant d'initiatives qui s'inscrivent dans une logique de *Zero Trust* sans en porter explicitement le nom. Cela explique pourquoi certaines organisations ont déjà réalisé des avancées significatives sans en faire un projet structuré.

LA RATIONALISATION ET LA CONVERGENCE DES OUTILS

Un des défis du *Zero Trust* réside dans la nécessité d'éviter un empilement d'outils hétérogènes qui complexifierait la gestion et l'orchestration des contrôles de sécurité. L'objectif est de casser les silos et de tendre vers une vue unifiée de la posture de sécurité, notamment à travers l'utilisation de data lakes de sécurité et de solutions convergentes.

L'unification des sources de données et l'adoption de solutions intégrées permettent de renforcer la cohérence des politiques de sécurité tout en optimisant les coûts et la gestion des incidents.

L'IMPORTANCE DU BASTION ET DES ACCÈS ADMINISTRATEURS

Le bastion d'administration reste un outil clé dans une approche *Zero Trust*, en particulier pour la gestion des accès administrateurs et des comptes à privilèges. Il permet de sécuriser ces accès critiques en appliquant des règles strictes d'authentification et de supervision. Toutefois, il ne constitue qu'un élément parmi d'autres et doit être intégré dans une approche globale de gestion des identités et des accès.

Défis et perspectives

UNE MISE EN ŒUVRE PROGRESSIVE ET ADAPTÉE AU CONTEXTE

L'adoption du *Zero Trust* varie fortement d'une organisation à l'autre en fonction de son niveau de maturité et de ses priorités en matière de cybersécurité. Si certaines organisations ont structuré un programme dédié, d'autres avancent de manière plus pragmatique en intégrant progressivement les principes du *Zero Trust* dans leurs stratégies existantes.

La difficulté d'inventaire et de classification des assets constitue un frein majeur à la mise en œuvre de certaines briques du *Zero Trust*, notamment le ZTNA. Une approche basée sur la conformité et les besoins métier peut être un bon levier pour progresser efficacement.

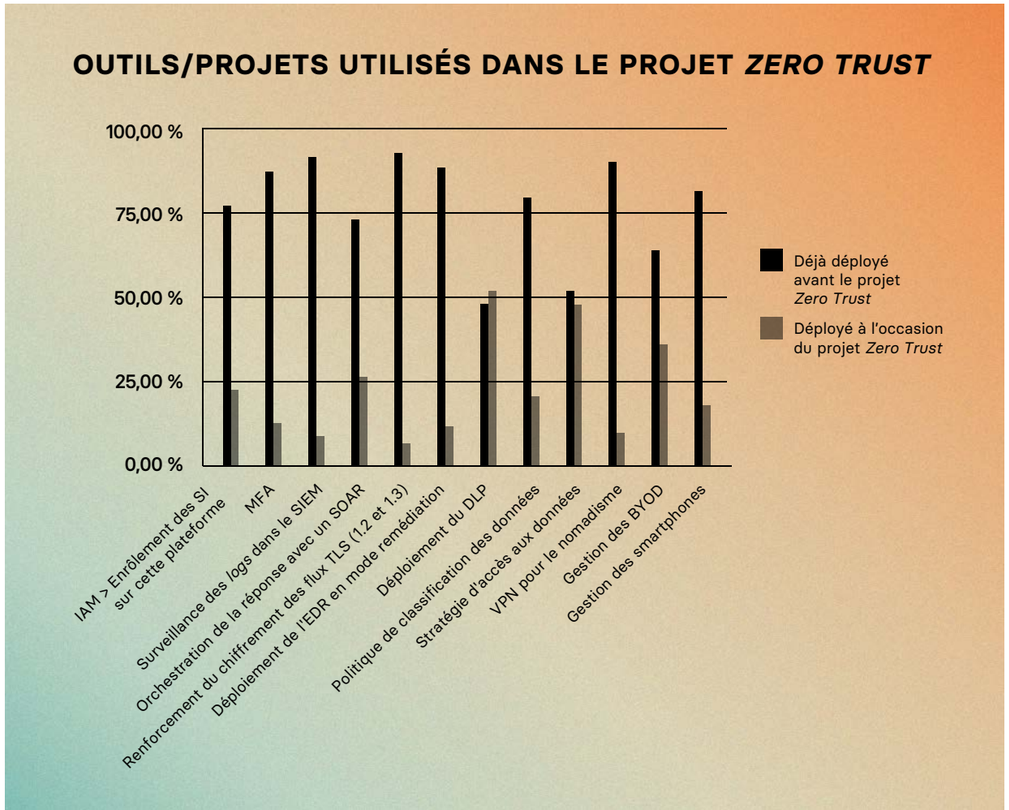
LE RÔLE DES NOUVELLES TECHNOLOGIES : ENTRE AVANCÉES ET *BUZZWORDS*

Certaines technologies comme l'intelligence artificielle et le machine learning sont souvent mises en avant dans le discours marketing des éditeurs. Pourtant, les approches basées sur l'analyse comportementale et les modèles statistiques existent depuis plus de dix ans et ne sont pas spécifiques au *Zero Trust*. Il est donc essentiel de ne pas se laisser emporter par les effets d'annonce et de privilégier une approche pragmatique, axée sur l'amélioration concrète des contrôles de sécurité.

CE QU'IL FAUT RETENIR

Le *Zero Trust* repose sur un écosystème technologique diversifié, combinant IAM, micro-segmentation, surveillance des logs et rationalisation des accès. Toutefois, il ne s'agit pas d'un simple empilement d'outils, mais d'une transformation en profondeur des processus de sécurité.

L'adoption d'une stratégie *Zero Trust* nécessite une approche progressive et pragmatique, adaptée aux contraintes et à la maturité de chaque organisation.



7

QUELLE SONT LES RETOURS D'EXPÉRIENCE SUR LE *ZERO TRUST* ET QUELLES SONT LES FUTURES PERSPECTIVES ?

RETOUR D'EXPÉRIENCE ET PERSPECTIVES DES PROJETS *ZERO TRUST*

Le *Zero Trust* s'impose progressivement comme un modèle de sécurité universel, en réponse à la transformation numérique, à la mobilité accrue des utilisateurs et à l'essor du *Cloud*. Cependant, sa mise en œuvre soulève de nombreuses questions, notamment en matière de coûts, d'organisation et de choix technologiques. Les retours d'expérience des experts du domaine permettent de mieux comprendre les enjeux et les tendances de ces projets.

UNE TRANSITION VERS LA PLATEFORMISATION

La complexification des systèmes d'information pousse des organisations à rechercher une approche plus intégrée. La plateformisation s'impose comme une nécessité, permettant de réduire la dispersion des solutions et d'améliorer la cohérence des politiques de sécurité. Dans cette logique, les organisations tendent à combiner deux ou trois grandes plateformes couvrant des domaines spécifiques :

— **IAM (Identity and Access Management) :** unification des identités et des accès sous une seule solution pour simplifier la gestion des droits.

— **Sécurisation des terminaux :** une plateforme unique pour sécuriser les postes de travail, serveurs, SaaS et terminaux mobiles, professionnels ou personnels.

— **Sécurité réseau :** intégration des solutions de micro-segmentation, de *firewalling* avancé et de gestion des accès distants.

— L'adoption d'une approche plateforme plutôt que le maintien d'une multitude de solutions les meilleures de leurs catégories ou *best of breed* permet de renforcer l'efficacité et de réduire la complexité d'administration.

RÉDUCTION DU NOMBRE DE SOLUTIONS POUR UNE MEILLEURE COHÉRENCE

Le *Zero Trust* exige une vision globale et une cohérence dans le choix des outils. Une multiplication des solutions entraîne des surcoûts et des difficultés d'intégration. Ainsi, les organisations cherchent à rationaliser leur portefeuille technologique afin de faciliter le déploiement et l'administration de la sécurité *Zero Trust*.

L'intégration des solutions joue un rôle clé : certaines technologies, comme certains pare-feu, permettent désormais d'activer des fonctionnalités de *Zero Trust* (comme des analyses comportementales avancées) par simple paramétrage, sans nécessiter de nouveaux investissements massifs.

LES COÛTS DU *ZERO TRUST :* UN INVESTISSEMENT STRATÉGIQUE

Si la mise en place du *Zero Trust* engendre des coûts initiaux, ils doivent prendre en compte les aspects suivants :

— **Paramétrage et configuration :** bien que l'initialisation puisse être complexe, certaines solutions permettent une activation rapide de fonctionnalités avancées.

— **Changement des processus :** l'un des coûts majeurs du *Zero Trust* réside dans l'adaptation des processus métiers et IT, bien plus que dans l'achat de nouvelles solutions technologiques.

— **Coût des exceptions :** la gestion des dérogations, notamment pour les dirigeants ou certaines fonctions critiques, peut être chronophage et nécessiter des ressources dédiées.

La mise en œuvre du *Zero Trust* peut servir de catalyseur pour renforcer des mesures de sécurité supplémentaires, telles que la réalisation d'analyses de risques pour les projets numériques au sein d'un grand groupe. Sans cette évaluation, la solution en question ne peut pas accéder aux ressources réseau. Ce processus permet non seulement de renforcer la sécurité, mais aussi d'améliorer la gouvernance des projets numériques.

UN PROJET STRUCTURANT, AU-DELÀ DE LA SEULE CYBERSÉCURITÉ

Le *Zero Trust* est parfois perçu comme un projet purement technologique ou comme un simple *buzzword*. Il est possible de le considérer comme un programme structurant nécessitant une approche transverse entre IT, métiers et gouvernance.

Le rôle du RSSI/CISO est central dans le cadre des projets *Zero Trust* :

— Définir une gouvernance claire et adaptée aux spécificités de l'organisation.

— Coordonner les différentes équipes IT impliquées dans la mise en place des contrôles.

— Sensibiliser les parties prenantes aux bénéfices et aux contraintes du *Zero Trust*.

Toutefois, la mise en œuvre d'un programme *Zero Trust* à grande échelle nécessite un soutien au plus haut niveau de l'organisation. Sans validation de la direction générale et sans allocation budgétaire adaptée, il est difficile d'obtenir les ressources nécessaires.

UN PROJET PROGRESSIF ET ÉVOLUTIF

Le *Zero Trust* ne se met pas en place du jour au lendemain. Son implémentation suit généralement une approche progressive :

1. **Définition d'une politique de sécurité claire, avec des objectifs et un cadre d'action.**
2. **Priorisation des chantiers, en commençant par des aspects critiques comme la gestion des identités.**
3. **Déploiement en vagues successives, pour éviter des changements brutaux et irréalistes.**
4. **Évaluation et ajustement continus, afin de s'adapter aux évolutions technologiques et aux besoins métiers.**

L'adoption massive du *Cloud* et des hyperviseurs conduit à une dépérimétrisation du Système d'Information, faisant du *Zero Trust* comme une solution incontournable, que ce soit de manière volontaire ou contrainte. Dès la conception des infrastructures, l'intégration des principes du *Zero Trust* simplifie l'adoption et évite des restructurations coûteuses a posteriori.

VERS UNE CONVERGENCE ENTRE IDENTITÉ ET RÉSEAU

L'avenir du *Zero Trust* semble se diriger vers une fusion progressive des solutions de gestion des identités et des solutions de sécurité réseau. L'objectif est d'obtenir une visibilité et un contrôle intégrés sur les utilisateurs, les ressources et les flux de données.

Cette convergence facilitera :

— Une gestion centralisée des accès et des permissions.

— Une réduction de la complexité opérationnelle.

— Une amélioration de la réactivité face aux menaces.

Les organisations ayant déjà adopté une approche *Zero Trust* témoignent souvent d'un gain significatif en sécurité et en résilience. En réduisant la surface d'attaque et en adoptant une posture proactive, elles minimisent les risques liés aux cybermenaces tout en améliorant la conformité réglementaire.

CE QU'IL FAUT RETENIR

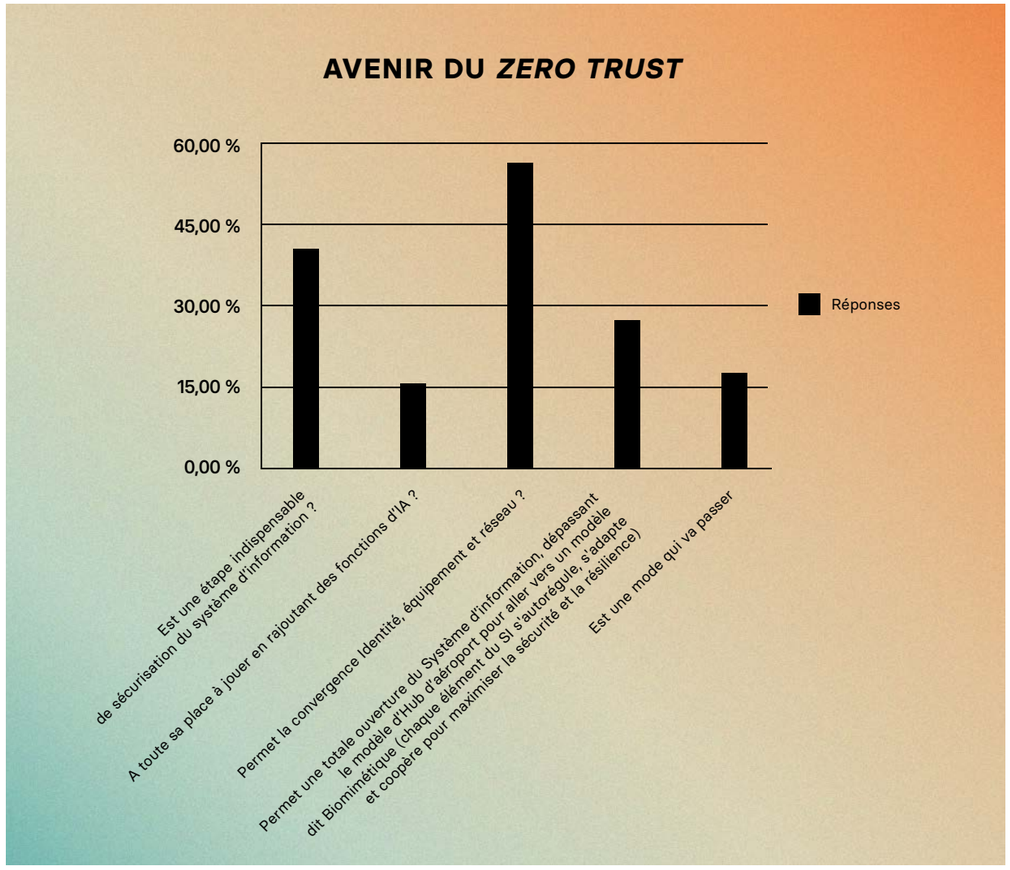
Le *Zero Trust* n'est pas un projet ponctuel mais une transformation profonde, à la fois sur les aspects appréhension des risques et techniques, de la manière dont la sécurité est pensée, mise en œuvre et maintenue. S'il nécessite un investissement initial important, il génère des bénéfices tangibles en matière de protection des données, de gestion des risques et d'optimisation des processus IT.

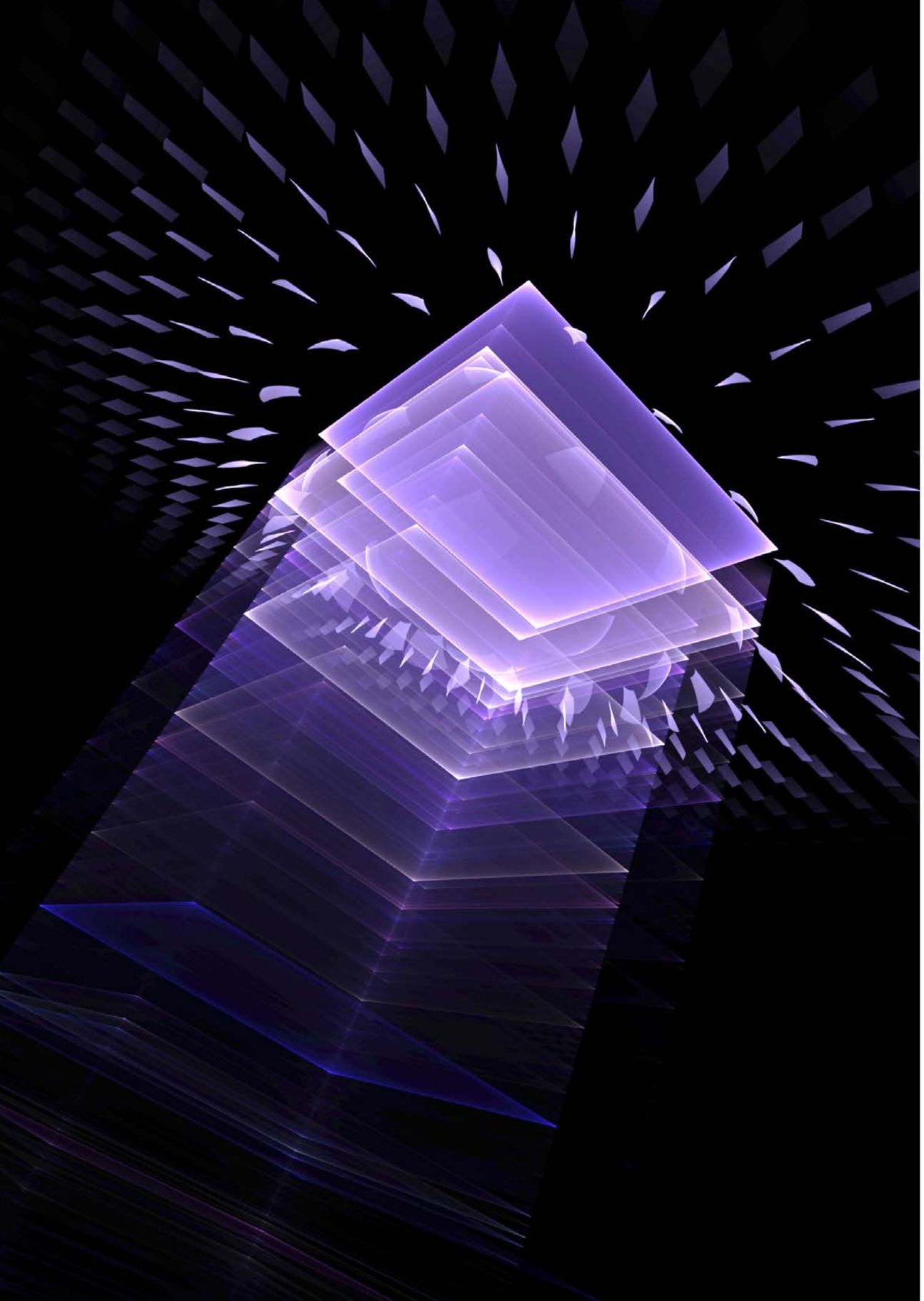
Les retours d'expérience montrent que l'approche plateforme, la rationalisation des solutions et une gouvernance claire sont des facteurs clés de succès.

« Il y a deux approches pour mener une transformation *Zero Trust*, soit faire du *Zero Trust* sans le savoir, lors de la configuration des différentes briques techniques d'infrastructures par exemple ou avoir un programme global de grande ampleur. »

Laurent BEAUPUIS

Klesia





8

GESTION DES TIERS ET ASPECTS JURIDIQUES DANS UNE APPROCHE

ZERO TRUST

L'intégration du *Zero Trust* doit être vue de manière holistique et prendre en compte l'écosystème de l'organisation. Dans ce contexte, la gestion des tiers et des aspects juridiques est une problématique complexe, notamment en raison de la diversité des acteurs impliqués et du niveau de maturité souvent hétérogène des relations avec les fournisseurs, sous-traitants et filiales. L'objectif est d'instaurer une confiance conditionnelle basée sur des principes de vérification continue et de classification rigoureuse des accès et des données.

LA MATURITÉ DES CONNEXIONS TIERCES : UN POINT FAIBLE

L'organisation étend naturellement son périmètre de sécurité à travers son écosystème de partenaires et de fournisseurs. Cependant, l'intégration des principes du *Zero Trust* se heurte à un obstacle majeur : la faible maturité des connexions avec les tiers. Les niveaux d'accès doivent être contrôlés en fonction de critères de confiance, définis par des prérequis techniques et organisationnels. Cette approche implique :

— Une classification rigoureuse des données et des actifs associés à chaque tiers.

— Un plan d'assurance sécurité (PAS) formalisant les exigences cyber imposées aux prestataires.

— Une validation continue des dispositifs de sécurité des partenaires, avec des contrôles fréquents.

— Un enregistrement des accès et des dérogations éventuelles avec un monitoring continu.

Les filiales posent une problématique similaire. Elles doivent être intégrées à la gouvernance *Zero Trust* selon des critères précis, en définissant un « poste de travail de confiance » conforme aux exigences du groupe.

L'IMPACT DU *ZERO TRUST* SUR LES SERVICES ET LES USAGES

L'évolution des architectures informatiques et des modes de travail (mobilité, télétravail, BYOD) complexifie davantage la gestion des tiers. L'ouverture du SI aux terminaux personnels et aux partenaires implique :

— Un processus d'enrôlement rigoureux des terminaux.

— Une surveillance continue de la conformité des équipements.

— Une adaptation des niveaux de service en fonction des politiques *Zero Trust* appliquées.

L'impact du *Zero Trust* est particulièrement fort sur les environnements les moins sécurisés, notamment les sous-traitants, qui disposent rarement des capacités techniques et financières nécessaires pour se conformer aux exigences élevées de sécurité.

INTÉGRATION DU *ZERO TRUST* DANS LES PROCESSUS D'ASSURANCE ET DE CONFORMITÉ RÉGLEMENTAIRE

L'un des leviers pour imposer une approche *Zero Trust* aux tiers repose sur les questionnaires d'évaluation des cyberassurances. De plus en plus, les assureurs évaluent la maturité *Zero Trust* des organisations afin d'ajuster leurs primes et garanties. Ce *scoring* peut :

— Aider les organisations à structurer leur inventaire des tiers et des accès associés.

— Encourager les partenaires à renforcer leur posture cyber pour éviter des exclusions de couverture.

— Apporter une incitation économique à l'application stricte des principes *Zero Trust*.

Par ailleurs, la pression réglementaire grandissante avec des réglementations comme DORA ou NIS2 incite les organisations à mieux structurer leur gouvernance cyber et à inclure leurs tiers dans cette démarche. Ces obligations peuvent aider à surmonter la réticence des prestataires, en particulier ceux avec une relation historique de plusieurs années, qui pourraient percevoir le *Zero Trust* comme une contrainte excessive.

SCORING ET ÉVALUATION DE LA POSTURE DE SÉCURITÉ DES TIERS

Les modèles de scoring externes, utilisés notamment par les cyberassureurs, comportent encore des limites. Ils manquent souvent de visibilité sur la posture réelle des partenaires et ne prennent pas toujours en compte les spécificités de chaque relation d'affaires. Des approches plus pertinentes incluent :

— L'usage de méthodes d'Analyse de Risques (EBIOS RM par exemple)

— L'utilisation de solutions de monitoring interne, type Managed Security Evaluation Model (MSEM), pour une visibilité plus fine.

— Une vérification systématique de la posture des terminaux des sous-traitants, bien que cette approche soit encore immature et oblige souvent à fournir des bureaux virtuels sécurisés.

— Une intégration progressive des exigences *Zero Trust* dans les appels d'offres et les contrats fournisseurs.

COMMUNICATION ET ACCOMPAGNEMENT DU CHANGEMENT

Le *Zero Trust* peut être perçu comme une contrainte excessive par certains partenaires, notamment ceux en relation de longue durée avec l'organisation. Une stratégie de communication ciblée est essentielle pour :

— Expliquer les bénéfices du modèle *Zero Trust* pour toutes les parties prenantes.

— Accompagner les fournisseurs dans la mise en conformité.

— Démontrer que l'approche *Zero Trust* simplifie, plutôt que complexifie, la gestion des relations contractuelles et techniques.

Enfin, il est important d'intégrer la Direction des Achats et la Direction Juridique dans cette transformation afin d'ancrer les principes *Zero Trust* dans les négociations contractuelles et d'assurer une cohérence globale.

En synthèse, l'intégration du *Zero Trust* dans la gestion des tiers et des aspects juridiques représente une avancée stratégique majeure. Cette approche, bien que complexe à mettre en œuvre, permet d'élever le niveau de sécurité global tout en rationalisant les relations avec les partenaires. Le renforcement des évaluations via le scoring et l'implication des assureurs pourrait être un levier de transformation efficace, à condition que les organisations accompagnent leurs tiers dans cette évolution. La pression réglementaire croissante jouera également un rôle clé en faveur de l'adoption massive du *Zero Trust* au sein des écosystèmes.

« L'application du *Zero Trust* peut complexifier les relations avec les fournisseurs. Elle doit être formalisée dans le cadre d'un Plan d'Assurance Sécurité. »

Michel DUBOIS

La Poste

CONCLUSION : LE
ZERO TRUST
UN NOUVEAU PARADIGME.

Face à l'ouverture des systèmes d'information, à la transformation numérique et aux nouvelles exigences réglementaires, Le *Zero Trust* apporte une approche pour conjuguer agilité, conformité et résilience.

L'essor du *Cloud,* du télétravail et des objets connectés (IoT) a considérablement élargi la surface d'attaque des organisations, rendant obsolète le modèle de sécurité périmétrique traditionnel, qui supposait le réseau interne comme une zone de confiance. Le *Zero Trust* répond à ces défis en adoptant un principe fondamental : « ne jamais faire confiance par défaut, toujours vérifier ». Chaque requête d'accès est évaluée dynamiquement en fonction de son contexte, limitant ainsi les risques de compromission et de propagation latérale des attaques, notamment grâce à la micro-segmentation.

Au-delà de la protection des actifs numériques, le *Zero Trust* peut être perçu comme accélérateur de transformation digitale. Il permet aux organisations de :

— Déployer des services *Cloud* et SaaS en toute sécurité, sans dépendre d'un périmètre réseau figé.

— Faciliter le travail hybride, en garantissant un accès sécurisé aux applications, où que se trouve l'utilisateur.

— Sécuriser les interactions avec les fournisseurs et partenaires, en appliquant des restrictions d'accès strictes aux seules ressources nécessaires.

Dans cette approche, le smartphone joue un rôle clé en tant que facteur d'authentification forte. Souvent utilisé aussi bien à des fins professionnelles que personnelles, sa compromission représente un risque majeur, car il peut devenir un vecteur d'attaques. Préserver son intégrité est essentiel pour garantir la fiabilité des processus d'authentification et de contrôle d'accès. Cela nécessite une gestion rigoureuse des terminaux, une adoption croissante de l'authentification sans mot de passe, ainsi qu'une surveillance continue des comportements suspects. L'isolation des environnements professionnels sur les dispositifs personnels devient également une mesure clé pour limiter les risques.

En définitive, le *Zero Trust* ne se réduit pas à une simple évolution technique : il s'agit d'une transformation stratégique qui redéfinit la cybersécurité comme un moteur de résilience et de performance. Ce nouveau paradigme permet aux organisations d'innover de manière agile, en sécurisant l'ensemble des interactions numériques et tout en soutenant leurs objectifs de croissance et de compétitivité.

« Le smartphone joue un rôle clé en tant que facteur d'authentification forte et sa sécurisation est clé dans le cadre d'une approche *Zero Trust* »

Philippe LATOMBE

Député de la première circonscription de la Vendée

ZERO TRUST

LE NOUVEAU PARADIGME

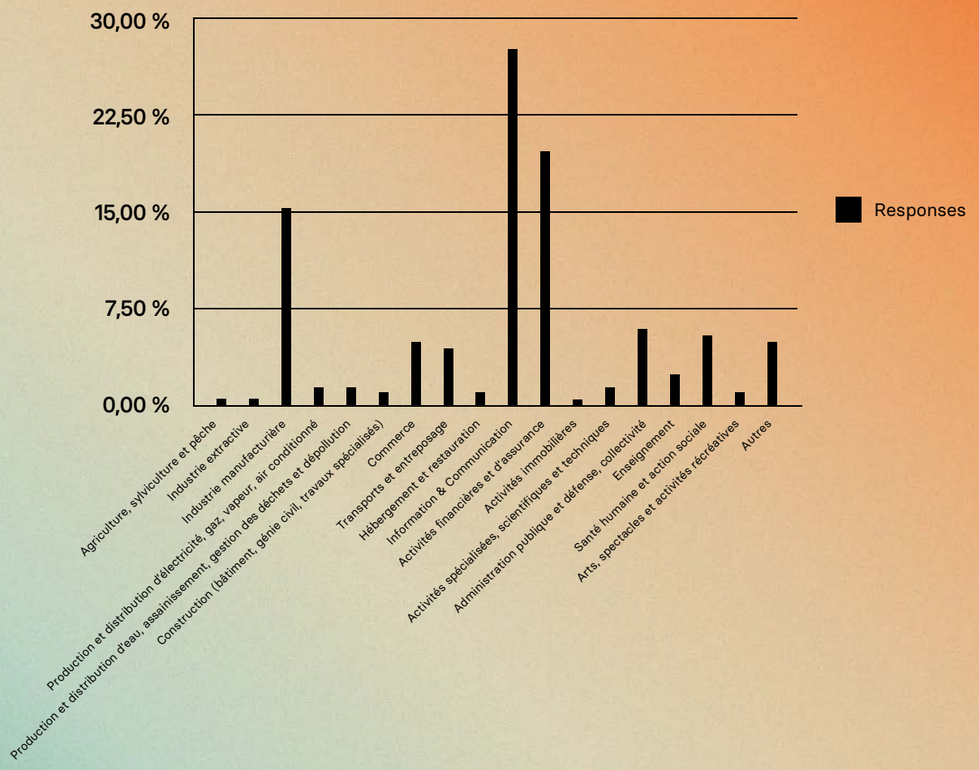
ANNEXES

Sondage du CESIN sur le *Zero Trust*

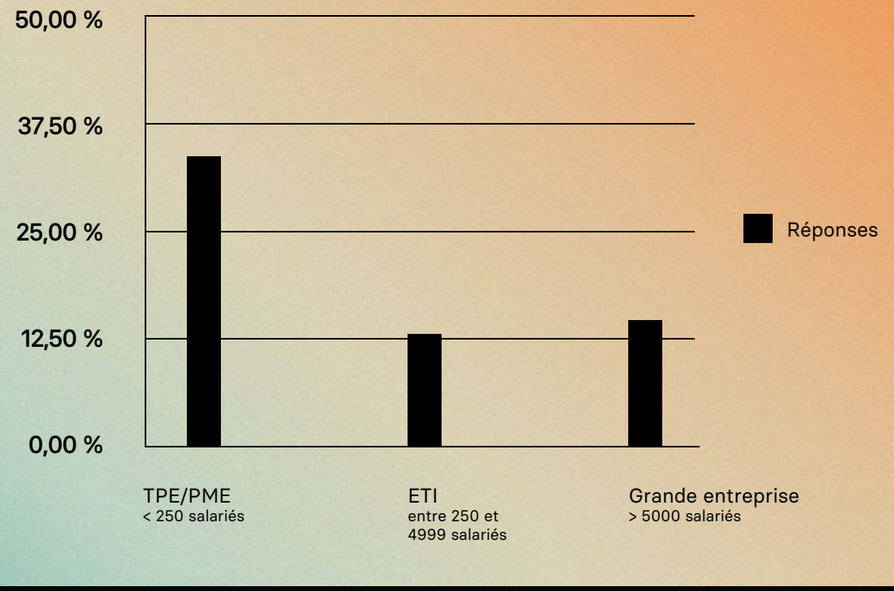
Ce livre blanc s'appuie sur une enquête menée auprès de 200 membres du CESIN, offrant un aperçu des tendances et perceptions du *Zero Trust* en 2025 selon des experts en sécurité des systèmes d'informations.

Nous remercions chaleureusement tous les participants pour leur contribution précieuse.

SECTEUR D'ACTIVITÉ



TAILLE ENTREPRISE



2025

IN CYBER
FORUM
EUROPE

ZERO TRUST

LE NOUVEAU PARADIGME

en partenariat avec

CESIN