TRIBUNE

Clichy, le 19 janvier 2026

LE RESEAU INTERNE, ANGLE MORT DU ZERO TRUST

Par Yann Bruneau, Chief Solutions Officer, Squad Cybersolutions

Le principe du Zero Trust semble limpide : ne jamais faire confiance, toujours vérifier. Ce modèle s'est imposé comme un standard de sécurité pour les organisations modernes. Mais dans la réalité du terrain, il s'arrête trop tôt : encore trop souvent réduit à sa seule dimension d'accès distant, il s'efface dès qu'on franchit le périmètre interne. Résultat : une sécurité à deux vitesses, et des zones d'ombre qui continuent de menacer la résilience des entreprises.

Un modèle universel mal appliqué

Beaucoup d'organisations ont déployé des solutions de ZTNA pour remplacer leurs VPN, renforcer leurs politiques d'authentification multifacteur et moderniser leurs annuaires d'identités. Des avancées réelles, certes, mais qui ne règlent qu'une partie du problème.

Une fois dans le réseau interne, les utilisateurs, humains ou machines, contrôlés par des mécanismes de sécurité éculés, bénéficient encore d'une confiance implicite. On continue de considérer le LAN comme une zone "sûre", alors que les menaces modernes se propagent en interne.

Le mouvement latéral reste l'un des vecteurs d'attaque les plus sous-estimés : un compte compromis, un endpoint infecté ou un équipement mal isolé peuvent permettre à un acteur malveillant de se déplacer sans entrave entre serveurs, applications ou environnements.

En d'autres termes, le Zero Trust s'arrête souvent là où il devrait justement commencer : au cœur même des infrastructures internes.

Les trois piliers d'un Zero Trust cohérent

Pour atteindre une posture de sécurité réellement cohérente, il faut s'appuyer sur trois piliers complémentaires :

- **L'identité comme fondation**

La gestion des identités est le socle du Zero Trust. Chaque accès, chaque connexion, chaque flux doit être associé à une identité vérifiée et continuellement évaluée. Cela suppose une gouvernance rigoureuse des identités humaines (IAM) et non-humaines (workload identities, comptes de service), une authentification forte systématique, et une analyse continue du contexte et des comportements. L'identité devient le nouveau périmètre : sans elle, aucune politique de confiance ne peut tenir.

- **Le contrôle d'accès universel**

Le Zero Trust exige une politique de contrôle uniforme, quel que soit le point d'accès, la localisation ou le type d'utilisateur. Les technologies d'Universal ZTNA permettent d'étendre cette logique au-delà

des accès distants : sièges, agences, sites industriels, clouds et interconnexions doivent être traités avec la même rigueur. Cette approche supprime la frontière artificielle entre "remote" et "on-premise", et renforce la visibilité sur l'ensemble des connexions.

- **La micro-segmentation pour limiter la propagation**

La brique la plus souvent négligée reste la micro-segmentation. Elle permet de limiter la surconnectivité interne, de restreindre les flux à ce qui est strictement nécessaire, et d'isoler les environnements critiques (OT, data centers, workloads cloud, etc.). Cette granularité transforme profondément la posture de sécurité : les flux deviennent explicites, la visibilité est complète, et chaque communication peut être analysée, vérifiée et consignée.
Ces trois piliers forment un tout indissociable : l'identité vérifie "qui", le contrôle d'accès détermine "quoi" et "où", et la micro-segmentation contraint "comment".

Changer de paradigme : du modèle de segmentation réseau au modèle de confiance
Mettre en œuvre un Zero Trust cohérent, ce n'est pas une affaire d'outils, c'est un changement de paradigme.

Il s'agit de passer d'une logique de topologie réseau à une logique de modèle de confiance. Plus question de seulement raisonner en VLAN, zones DMZ ou segments "internes" : chaque flux doit être justifié, chaque communication explicitement autorisée, indépendamment de sa provenance topologique.

Cette transformation exige une cartographie fine des dépendances applicatives, une connaissance précise des flux métier, et une collaboration renforcée entre les équipes sécurité, réseau, identités et opérations. Ce n'est qu'à cette condition que l'on peut construire des politiques de confiance granulaires, basées sur le contexte réel des échanges et non sur des présomptions héritées de l'architecture physique.

Conclusion
Le Zero Trust n'est pas un produit ni une norme : c'est un cadre d'architecture, une philosophie opérationnelle.

Tant que les organisations continueront de tracer une frontière entre "extérieur" et "intérieur", elles resteront vulnérables aux menaces les plus pernicieuses.

Un Zero Trust universel, qui articule identité, contrôle d'accès et segmentation, n'est pas seulement un idéal technique : c'est une condition sine qua non de résilience face à des attaques toujours plus furtives et dynamiques.

Chez Squad Cybersolutions, nous défendons cette vision exigeante : celle d'un Zero Trust qui ne s'arrête pas à la porte du réseau, mais qui s'applique à chaque identité, chaque connexion, chaque flux, et chaque instant.

A propos de Squad Cybersolutions

Squad Cybersolutions, ex Newlode, est intégrateur et Managed Security Service Provider (MSSP), expert des enjeux de cybersécurité. Filiale du Groupe Squad depuis fin 2023, Squad Cybersolutions accompagne la sécurisation des infrastructures IT & OT de ses clients, de la phase conseil au pilotage automatisé multi-éditeurs de leurs architectures. Sa force, c'est sa capacité à construire et déployer des environnements intelligents capables d'optimiser leur défense face aux menaces. Opérant pour la moitié du CAC 40 et du SBF 120, Squad Cybersolutions pilote des projets Build/Run d'envergure internationale et dispose d'un Operation Center parisien qui officie en

24x7 et repose sur une équipe d’experts, capables de s’engager sur des SLA clients exigeants. Avec 1000 collaborateurs en France et à l'International, le Groupe Squad réalise 125 millions d'euros de chiffre d'affaires.

Contacts presse
Franck Tupinier
MyNTIC PR
ftupinier@myntic-pr.com

Lily Magagnin
CMO Squad Group
lily.magagnin@squadgroup.com