ARP GUARD by ISL

WHITEPAPER

# ZERO-TRUST
Network Access

SecurITy made in Germany

Trust Seal www.teletrust.de/itsmig

## LA CONFIANCE C'EST BIEN - LE ZERO-TRUST C'EST MIEUX

### UN CONCEPT DE SÉCURITÉ INFORMATIQUE RÉSILIENT

Les modèles de sécurité traditionnels situent généralement l'attaquant potentiel en dehors des limites du propre réseau. Ainsi, les vulnérabilités de sécurité causées par les composants du réseau ou les droits d'accès au sein du réseau sont souvent négligées. Les stratégies de sécurité qui protègent les entreprises principalement contre les accès de l'extérieur, ne peuvent plus résister suffisamment aux défis actuels de la cybercriminalité comme le Social Engineering et les attaques de phishing. La multiplication des attaques lancées depuis le réseau, rendent nécessaire une couche de protection supplémentaire et exigent des concepts de sécurité globaux et résilients qui réagissent de manière ciblée à la situation de sécurité existante afin de pouvoir répondre aux exigences qui en résultent.

### ZERO-TRUST NETWORK ACCESS

Avec la solution ARP-GUARD Network Access Control l´entreprise ISL GmbH a mis en place dès 2003 une approche de sécurité fondamentale qui est de plus en plus essentielle de nos jours.

La solution ARP-GUARD NAC mise sur le contrôle permanent de tous les accès et identifie de manière univoque chaque appareil avant qu'il n'accède au réseau et aux ressources. Une approche qui est aujourd'hui connue sous le nom de „Zero-Trust Network Access". (ZTNA).

### NE FAIS JAMAIS CONFIANCE - VÉRIFIE TOUJOURS

Selon ce principe de base d'un concept de sécurité avancé, aucun appareil n'est fiable par défaut, même s'il se trouve à l'intérieur du réseau. Chaque tentative d'accès est systématiquement contrôlée et consignée - l'accès n'est accordé qu'après une authentification réussie. Avec ARP-GUARD NAC, vous disposez de deux éléments essentiels au niveau de l'appareil et du réseau pour un concept résilient de Zero Trust, qui peut être facilement étendu pas à pas avec d'autres modules fonctionnels.

Une visibilité maximale pour une protection maximale contre les menaces. ARP-GUARD fournit une vue immédiate et complète de tous les actifs du réseau.

ARP-GUARD propose un ensemble complet de règles dans lequel vous pouvez définir des directives à l'échelle de l'entreprise et définir des politiques personnaliser. Contrôlez quelles ressources sont accessibles à qui et protégez les données et les ressources sensibles contre tout accès non autorisé.

En surveillant en permanence l'activité du réseau, ARP-GUARD fournit une vue d'ensemble sur tout ce qui se passe sur votre réseau en temps réel. Les accès non souhaités et les anomalies remarquables sont identifiés précocement et le niveau de sécurité de votre réseau est augmenté de manière significative.

La micro segmentation du réseau limite énormément les possibilités de la liberté de mouvement d'un agresseur potentiel. La propagation ainsi que les dommages causés sont ainsi drastiquement réduites et contrôlables.
L'attribution s'effectue de manière dynamique grâce à la gestion VLAN d'ARP-GUARD, des directives de sécurité à granularité fine pour les différents segments du réseau peuvent être définies de manière spécifique dans le système de règles.

ARP-GUARD Endpoint vérifie avant l'accès à l'appareil au réseau, si l'appareil utilisé remplit les conditions préalables telles que les exigences de conformité ou de sécurité dans le réseau.

ARP-GUARD identifie de manière univoque chaque appareil avant qu'il n'ait accès au réseau. L'authentification forte par empreinte digitale protège contre les manipulations de réseau telles que l'usurpation d'adresse MAC (MAC SPOOFING) ou ARP POISONING.

**Comment expliquer Zero Trust aux cadres dirigeants?**

Il s'agit de la construction d'une architecture qui ne fait jamais confiance aux connexions, qui les vérifie toujours et qui part du principe qu'un acteur malveillant peut être actif à tout moment, ce qui se traduit par une grande résilience et des environnements système très flexibles, bien mieux adaptés aux exigences du lieu de travail moderne.

*Source: www.gartner.com*