ARP GUARD by ISL

SERVICE

CLIENT-GUARD

Network Access Control

SecurITy made in Germany

Trust Seal www.teletrust.de/itsmig

LA RÉVOLUTION DU CONTRÔLE D'ACCÈS AU RÉSEAU

LES DÉFIS DES TERMINAUX DÉLOCALISER

La gestion de l'accès au réseau constitue un défi majeur, en particulier dans le contexte de la tendance croissante au travail en tout lieu. Jusqu'à présent, l'intégration d'appareils externes, par exemple depuis le bureau à domicile via VPN, dans l'infrastructure réseau constituait un défi particulier en termes de respect des directives de conformité.

CLIENT-GUARD, UN NOUVEAU STANDARD POUR UNE CONFORMITÉ INTÉGRALE

Pour renforcer la résilience du réseau de l'entreprise, principalement dans les situations où les terminaux sont utilisés en dehors du réseau de ce dernier, un niveau de sécurité accru est nécessaire afin de minimiser les risques pour l'ensemble de l'infrastructure informatique. Le CLIENT-GUARD établit un nouveau standard pour le respect des directives de conformité pour les terminaux utilisés indépendamment de l'endroit où ils se trouvent. Il conserve toutes les fonctionnalités d'ARP-GUARD pour l'orchestration et l'application des politiques de conformité afin de garantir un niveau de sécurité maximal.

DEVICE INFORMATION & ACCESS CONTROL

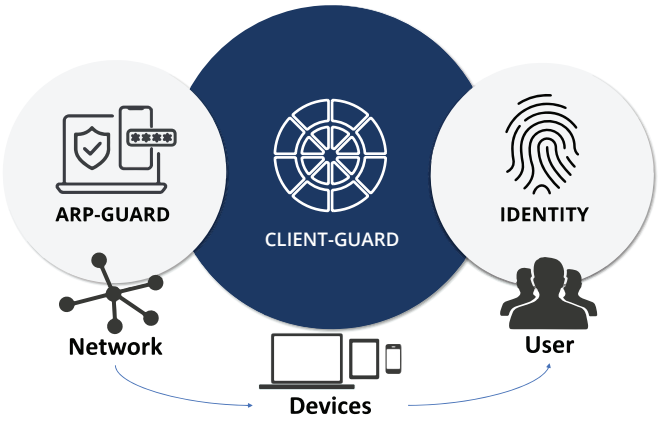
Le CLIENT-GUARD assume des fonctions importantes dans le domaine des informations sur les appareils et de la gestion du contrôle d'accès. Tout d'abord, il détermine l'identité des appareils connectés et collecte des informations complètes. Il s'agit notamment de collecter des données pour garantir le respect des directives relatives aux points finaux et l'état de conformité. Sur la base de ces informations, le CLIENT-GUARD peut effectuer différentes actions. Il a la capacité d'accorder ou de refuser l'accès au réseau pour les appareils, en fonction des politiques et des exigences de sécurité définies. La gestion centrale permet de déposer des ensembles de règles individuelles pour les points finaux. Il est ainsi possible de définir des exigences et des politiques de sécurité spécifiques pour chaque appareil du réseau.

TRANSPARENCE COMPLÈTE

Un contrôle de sécurité de base permet de s'assurer que les applications nécessaires et liées à la sécurité sont correctement installées et versionnées. Cela comprend, entre autres, les programmes anti-malware, les pares-feux, les logiciels de cryptage, les navigateurs web, les outils de communication et les VPN. En outre, des données telles que des informations sur l'utilisateur, des informations sur le système d'exploitation, une liste des applications installées, y compris le statut des certificats, sont fournies. Ces données permettent d'obtenir un aperçu complet des aspects de sécurité et de configuration de tous les appareils externes et de s'assurer qu'ils répondent aux normes de sécurité en vigueur.

LA VOIE VERS L'APPROCHE ZERO TRUST

Avec notre ARP-GUARD Network Access Control, notre CLIENT-GUARD et notre solution IDENTITY, nous vous préparons au ZERO TRUST. Avec ARP-GUARD NAC, la vérification de l'identité est effectuée par une technologie d'empreintes digitales propre ; chaque tentative d'accès est enregistrée en temps réel. Le CLIENT-GUARD tient compte de l'état et de la conformité des appareils en fournissant des informations contextuelles importantes. IDENTITY permet une autorisation d'accès basée sur le principe du „least privilege" et utilise des méthodes d'authentification forte à facteurs multiples pour renforcer encore la sécurité des accès et empêcher les accès non autorisés.



LES AVANTAGES DU CLIENT-GUARD EN UN COUP D'ŒIL

- Client „as a Service" ménageant et économisant les ressources à partir de centres de données certifiés et allemands
- Transparence et contrôle complets pour tous les terminaux à l'intérieur et à l'extérieur du réseau de l'entreprise
- Ensembles de règles définissables individuellement pour des directives de sécurité dédiées et des exigences de conformité
- En combinaison avec ARP-GUARD NAC et IDENTITY, la voie idéale vers le concept Zero-Trust