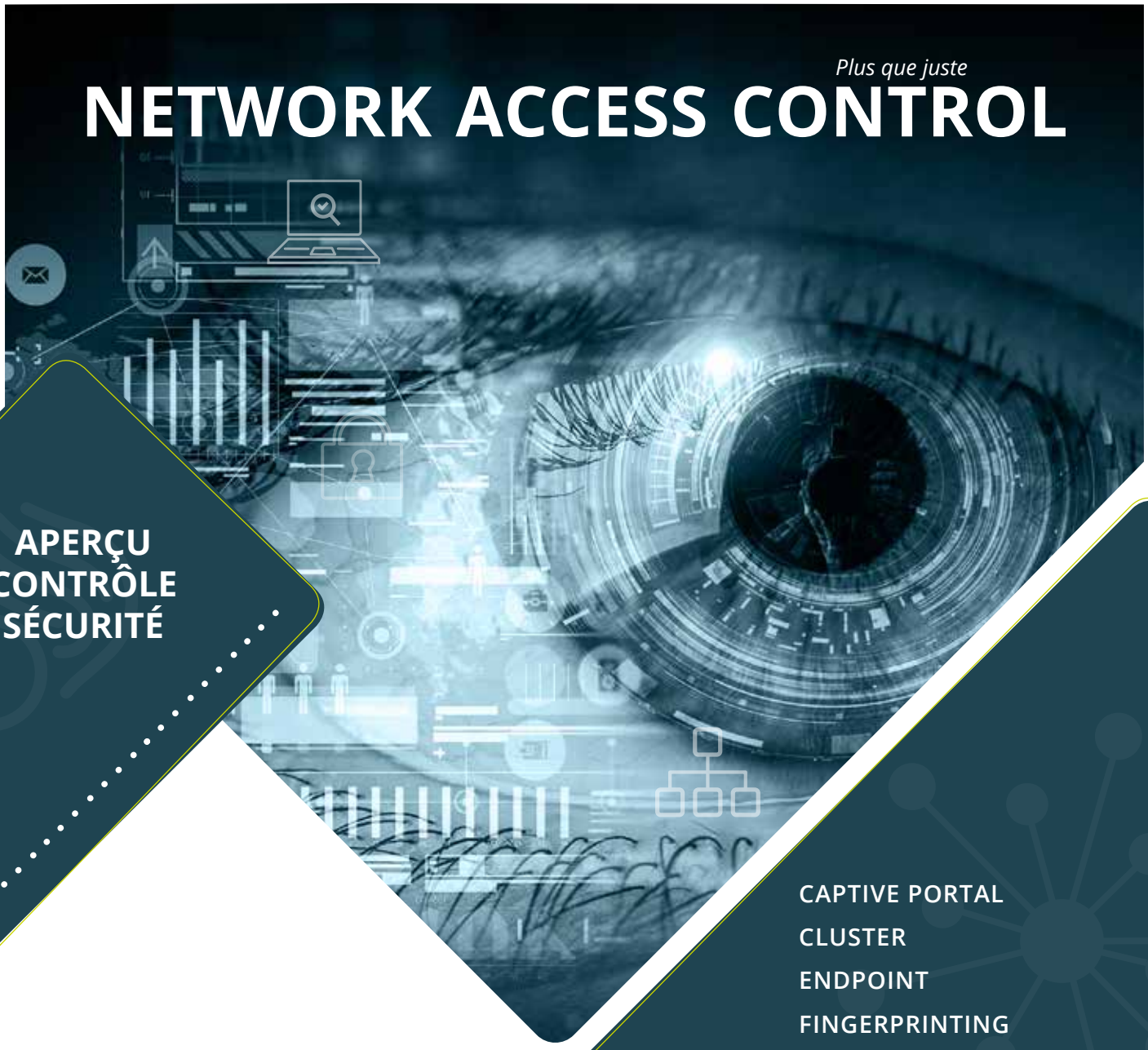
ARP GUARD by ISL

Plus que juste

NETWORK ACCESS CONTROL



APERÇU CONTRÔLE SÉCURITÉ

- CAPTIVE PORTAL
- CLUSTER
- ENDPOINT
- FINGERPRINTING
- DÉTECTION D'APPAREILS
- SENSOR-MANAGEMENTSYSTEM
- VLAN-MANAGER
- PROTECTION D'ACCÈS

ARP-GUARD est notre solution éprouvée de contrôle d'accès au réseau (Network Access Control - NAC) qui, contrairement aux applications réseau complexes et coûteuses, peut être facilement mise en œuvre même dans des réseaux hétérogènes et de grande taille. Avant qu'ils n'accèdent au réseau, la protection de l'accès identifie rapidement et sans ambiguïté les appareils connus et inconnus, quel que soit leur fabricant ou leur technologie. Au-delà de la norme de protection d'accès pure, la solution regroupe également les informations relatives à la sécurité sous forme d'instance centrale, détecte et signale les anomalies dans le réseau et les corrige immédiatement.

SecurITy made in Germany

Trust Seal
www.teletrust.de/itsmig

LA SOLUTION ARP-GUARD EN DÉTAIL

DÉTECTION ET INVENTAIRE DES APPAREILS

ARP-GUARD communique avec l'ensemble de l'infrastructure du réseau et détecte tous les systèmes qui s´y trouve en un temps très court. Chaque appareil final devient visible et les sources d'interférence peuvent être rapidement localisées et éliminées. En outre, la solution présente l'ensemble de l'architecture dans une topologie graphique. Non seulement cela facilite la planification du réseau, cela permet d'atteindre la transparence requise par les audits et les révisions.

PROTECTION D'ACCÈS

Le contrôle et la régulation centralisés de tous les accès au réseau permettent un contrôle complet. Les appareils inconnus sont détectés et signalés en temps réel. Après l'identification claire, la procédure suivante a lieu. De l'arrêt immédiat d'un port à la relocalisation dans un réseau local virtuel (VLAN) dédié, toute action souhaitée peut être définie et gérée dans le jeu de règles pour l'ensemble du réseau.

SEGMENTATION DU RÉSEAU AVEC VLAN-MANAGER

Avec la gestion VLAN, la segmentation en VLAN peut être facilement mise en œuvre et gérée de manière pratique. Les zones sensibles font l'objet d'une protection supplémentaire, les zones publiques sont clairement séparées des zones internes et les invités et prestataires de services ne bénéficient que d'un accès spécial. Au lieu d'une configuration manuelle sur les différents ports du commutateur, l'affectation au VLAN associé est automatisée selon un ensemble de règles. Les employés qui déménagent, voyagent ou travaillent sur d'autres sites emportent toujours leur environnement avec eux.

FINGERPRINTING

La combinaison de différentes méthodes d'authentification, telles que RADIUS basé sur MAC et 802.1X, offre sécurité et flexibilité. Nous complétons ces méthodes par l'ARP-GUARD Fingerprinting. Il saisit diverses propriétés, telles que les certificats et les clés cryptographiques, afin d'identifier un appareil de manière véritablement unique.

SENSOR-MANAGEMENTSYSTEM

Grâce à l'architecture spéciale de gestion des capteurs, ARP-GUARD est capable de gérer plusieurs clients et il est extrêmement évolutif. L'utilisation de capteurs permet l'intégration efficace d'un nombre quelconque de sites. Enterprise-Management permet d'administrer des environnements réseau décentralisés et de grande taille. Un ensemble central de règles est réparti sur l'ensemble du réseau comme une protection, simple et automatisée. Les utilisateurs, les rôles, les droits et les politiques sont synchronisés. Cependant, des capteurs peuvent également être utilisés de manière décentralisée.

ARP-GUARD ADD-ONS

CAPTIVE PORTAL - ACCÈS INVITÉ & BYOD

L'add-on Captive Portal contrôle l'accès au réseau des invités et des composants tiers, par exemple les smartphones ou les ordinateurs portables. Dans chaque environnement, il est possible de définir un accès au réseau ciblé pour les appareils tiers, contrôlé à tout moment par un ensemble de règles de pare-feu dynamiques, grâce au capteurs de la gestion de l´architecture, cela est même possible entre les différents sites. Cela facilite la mise en œuvre du BYOD (Bring Your Own Device) et les appareils privés ne reçoivent qu'un accès explicitement autorisé par un ensemble de règles.

INTÉGRITÉ DU RÉSEAU SUR TOUS LES APPAREILS

La fonction Endpoint d'ARP-GUARD offre un soutien précieux à la mise en œuvre des exigences de conformité. Lors de l'authentification, il est vérifié si les appareils sont conformes aux directives de sécurité et s'ils le sont en ce qui concerne les détails relatifs à la sécurité, par exemple l'état, l'antivirus ou le niveau de correctif du système d'exploitation. Si les directives ne sont pas respectées, le dispositif est isolé et mis à jour dans un VLAN de quarantaine, par exemple. Ce n'est qu'après le contrôle ou l´ajustementle que les appareils reçoivent l'accès aux zones du réseau.

HAUTE DISPONIBILITÉ DE CLUSTER POUR LES SECTEURS INFORMATIQUES SENSIBLES

Le module complémentaire de cluster permet la réplication de serveurs avec des moyens logiciels et matériels simples pour une résilience et une évolutivité accrue des systèmes informatiques critiques.

ARP-GUARD EN BREF

- Détection et inventaire des appareils
- Contrôle et surveillance centralisés de l'accès au réseau
- Définition et application centralisées des directives en temps réel
- Segmentation du réseau
- Intégrité du réseau LAN/WLAN jusqu'aux équipements terminaux
- Fingerprinting unique pour une identification unique des appareils
- Contrôle de conformité des appareils
- Réglementation de l'accès des invités et BYOD
- Réduction de l'effort d'administration informatique grâce à l'automatisation
- Fabricant et technologie indépendants
- Prise en charge de ISO/IEC 27001, DIN EN 80001-1, PCI/DDS

VOS VALEURS AJOUTÉES

MISE EN ŒUVRE SIMPLE

Même avec une installation de base réussie, un niveau de sécurité nettement plus élevé est atteint, lequel peut être étendu étape par étape. L'intégration dans l'infrastructure existante est transparente et sans problème, sans qu'il soit nécessaire de procéder à des modifications ou à des investissements supplémentaires.

MISE À DISPOSITION

L´ARP-GUARD Management est fourni sous forme d'appliance virtuelle et physique. Avec une installation en cluster, il y a également la possibilité d'un fonctionnement mixte. En outre, des capteurs peuvent également être installés directement sur les serveurs de l'entreprise.

FORCES INTERSECTORIELLES

L´ARP-GUARD est utilisé dans tous les domaines. Outre l'industrie, le commerce, les soins de santé, les autorités publiques, l'enseignement et la recherche, la solution est particulièrement indispensable dans le secteur financier, l'un des secteurs les plus sensibles en matière de sécurité. La flexibilité, l'architecture et les fonctionnalités d'ARP-GUARD sont parfaitement adaptées aux infrastructures critiques (KRITIS). Le respect des exigences en matière de sécurité des normes ISO 27001 et DIN EN 80001-1, PCI/DSS ainsi que la certification sur le fondement de la protection de base IT sont pour nous une évidence.

COMBINAISON DE MÉTHODES POUR PLUS DE SÉCURITÉ ET DE FLEXIBILITÉ

L´ARP-GUARD couvre toute la gamme des possibilités d'authentification. Avec la version 4.0, l'interaction a mûri pour devenir une symbiose parfaite à l'état actuel du développement. La licence permet un fonctionnement mixte de SNMP, de RADIUS basé sur MAC et de 802.1X avec le même ensemble de fonctionnalités. Une migration ultérieure de SNMP vers 802.1X est également facile à réaliser.

SERVICE & SUPPORT

Nos partenaires qualifiés et expérimentés d'ARP-GUARD se feront un plaisir de vous soutenir en première instance dans toutes les situations problématiques et les questions d'assistance.
https://www.isl.de/fr/contact/partenaires-de-distribution

En outre, vous profiterez également de nos offres de service complètes : Abonnement au logiciel (accès à toutes les versions mineures et majeures, aux mises à jour ainsi qu'aux nouvelles versions), assistance de troisième niveau (assistance du fabricant pour l'optimisation et l'adaptation spécifiques au client), formation technique.Training.

SPÉCIFICATIONS

Plateformes de virtualisation

Les appliances virtuelles sont prises en charge sur

- VMware
- Microsoft Hyper-V
- KVM

Systèmes d'exploitation pris en charge

- Linux, Red Hat
- DOMOS
- CentOS
- Microsoft (Sensoren)

Méthodes d'authentification

- MAC-based RADIUS
- EAP
- SNMP
- 802.1X

Protocoles

- RADIUS
- SNMP
- SSH
- Telnet
- DHCP
- LDAP
- HTTPS
- Kerberos
- WMI

Navigateurs pris en charge

- Google Chrome
- Mozilla Firefox
- Safari
- Microsoft Internet Explorer
- Microsoft Edge