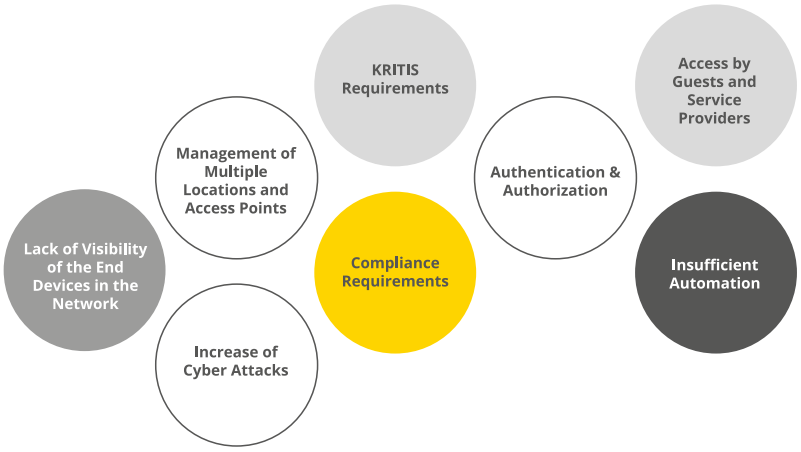
DTS

DTS
Network Access Control (NAC)

Network Access Control (NAC)

Von Unternehmensnetzwerken werden nicht nur ständige Verfügbarkeit, sondern auch durchgehende Sicherheit erwartet. Aber wie gewährleistet man eine zielgenaue Übersicht, Erkennung und Kontrolle? ARP-GUARD ist die führende Network Access Control (NAC) Lösung von den Spezialisten der ISL Internet Sicherheitslösungen GmbH. Die ISL ist ein anerkannter deutscher Software-Hersteller mit Fokus auf NAC. Im Gegensatz zu komplexen sowie teuren Anwendungen lässt ARP-GUARD sich in heterogenen und großen Netzwerken unkompliziert realisieren. Dabei setzt die Lösung neue Standards. Sie identifiziert, unabhängig von Herstellern oder Technologien, alle bekannten sowie unbekannten Geräte schnell und eindeutig, bevor diese einen Netzwerkzugang erhalten. Zudem bündelt ARP-GUARD sicherheitsrelevante Informationen, erkennt, meldet und korrigiert Anomalien im Netzwerk.

- Geräteerkennung & -inventarisierung
- Einzigartiges Fingerprinting zur eindeutigen Device-Identifizierung
- Maximale Sichtbarkeit, Kontrolle & Überwachung der Netzwerke
- Netzwerksegmentierung & -integrität bis zu den Endgeräten
- Identifizierung von Schwachstellen
- Zentrale Definition & Durchsetzung von Richtlinien in Echtzeit
- Schutz sensibler Daten & Bereiche sowie Compliance konforme Datensicherheit
- Aufwands- & Kostenreduzierung durch Automatisierung
- IT-Security „Made in Germany“ by DTS



BSI, KRITIS oder branchenspezifische Institutionen haben als gemeinsame Anforderung, dass ausschließlich autorisierte Systeme im Netzwerk zugelassen werden dürfen. Das Wichtigste ist hierbei der Leitspruch: „Sicherheit kommt durch Sichtbarkeit“. ARP-GUARD erkennt und inventarisiert die gesamte Netzwerkinfrastruktur innerhalb kürzester Zeit. Jedes Endgerät wird sichtbar und Störquellen lassen sich lokalisieren. Zudem stellt die Lösung die gesamte Architektur grafisch dar. Das erleichtert nicht nur die Netzwerkplanung. Es ermöglicht eine Transparenz, die z. B. von Audits und Revision gefordert wird.

Die zentrale Steuerung aller Netzwerkzugänge bietet einen umfassenden Zugangsschutz. Unbekannte Geräte sowie Statusveränderungen werden in Echtzeit erkannt und gemeldet. Nach der eindeutigen Identifizierung kann anschließend jedes Vorgehen per Regelwerk festgelegt und verwaltet werden - von der Portabschaltung bis zur Verlegung in ein spezielles Virtual Local Area Network (VLAN).

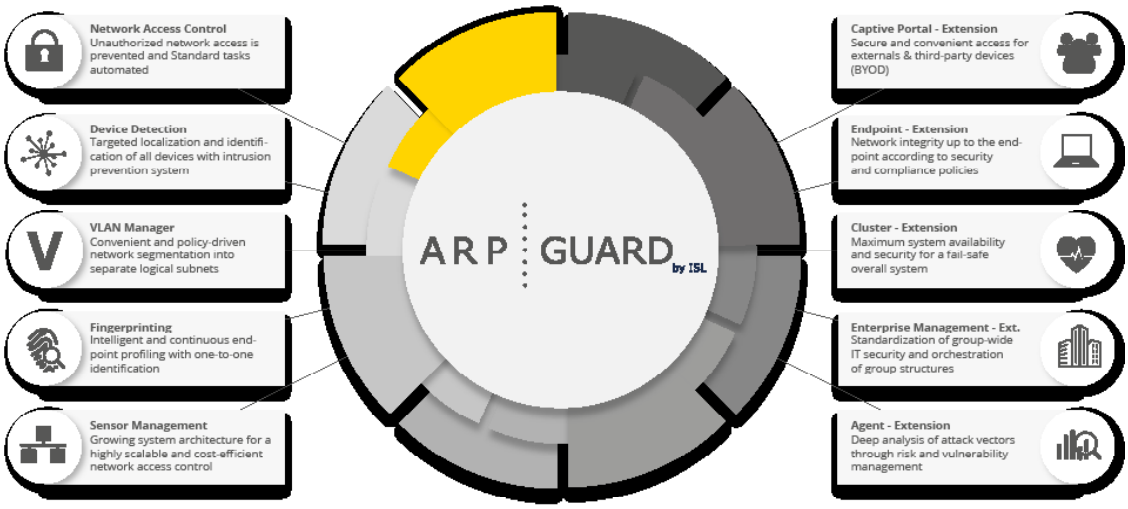
Mit dem VLAN-Management lässt sich die Netzwerksegmentierung in VLANs komfortabel umsetzen. Sensible Bereiche werden dadurch zusätzlich geschützt, öffentliche Bereiche klar von internen abgegrenzt und Gästen sowie Dienstleistern nur spezieller Zugang gewährt. Die Zuweisung in das zugehörige VLAN erfolgt automatisiert.

Die Kombination verschiedener Authentifizierungen, u. a. MAC-based RADIUS und 802.1X, bietet viel Sicherheit. Ergänzt werden diese Methoden durch das ARP-GUARD Fingerprinting. Es identifiziert Geräte durch verschiedene Eigenschaften wie kryptografische Zertifikate und Schlüssel eindeutig.

Durch die besondere Sensor-Management-Architektur ist ARP-GUARD mandantenfähig und enorm skalierbar. Das ermöglicht die Einbindung beliebig vieler Standorte. Das Umbrella-Management ermöglicht hierbei die Verwaltung dezentraler, großer Netzwerkumgebungen. Dabei ist ein zentrales Regelwerk wie ein Schirm über das gesamte Netzwerk ausgebreitet, simpel und automatisiert. Benutzer, Rollen, Rechte und Policies werden synchronisiert.

Das Captive Portal regelt den Netzwerkzugang von Gast- und Fremdkomponenten. In jeder Umgebung können für Fremdgeräte gezielte Zugänge definiert werden, jederzeit kontrolliert durch ein dynamisches Firewall-Regelwerk, auch standortübergreifend. Somit ist Bring Your Own Device (BYOD) einfach zu verwirklichen und die privaten Devices erhalten explizit freigegebene Zugriffe.

Das Endpoint Add-on liefert eine wertvolle Compliance-Unterstützung. Während der Authentifizierung wird geprüft, ob Endgeräte den Sicherheitsrichtlinien entsprechen und compliant sind, z. B. Status, Antivirus oder Patch-Level des Betriebssystems. Werden die Richtlinien nicht erfüllt, wird das Gerät isoliert und z. B. in einem Quarantäne-VLAN aktualisiert.



ARP-GUARD kommt in allen Bereichen zum Einsatz. Neben Industrie, Handel, Gesundheitswesen, Behörden, Bildung und Forschung, ist die Lösung vor allem im Finanzsektor, als einer der sicherheitssensibelsten Branchen überhaupt, nicht wegzudenken.

Das ARP-GUARD Management wird als virtuelle und physische Appliance zur Verfügung gestellt. Die Integration in die bestehende Infrastruktur erfolgt nahtlos. Bei einer Clusterinstallation besteht zudem die zusätzliche Möglichkeit eines Mischbetriebs. Außerdem können Sensoren direkt auf den unternehmenseigenen Servern installiert werden.

Unsere 4 ARP-GUARD Pakete:

ARP-GUARD Access – Netzwerkzugangsschutz:
RADIUS / 802.1X / EAP mit und ohne Zertifikat, MAC based RADIUS, MAC-Authentifizierung, benutzerdefiniertes Regelwerk, zentrales dynamisches Port-Security-System, Gäste-System mit Selbstregistrierung

ARP-GUARD Access+ – NAC & VLAN-Management:
Access zzgl. Abgrenzung von Netzwerksegmenten, dynamische und statische Zuordnung, kryptografisches Fingerprinting, Gäste-System mit Selbstregistrierung

ARP-GUARD Finance – Layer 2 IPS & NAC:
Access zzgl. Schutz vor Layer-2-Angriffen, Schutz vor fremden und unbekannten Geräten, kryptografisches Fingerprinting, Gäste-System mit Selbstregistrierung

ARP-GUARD Premium – All in One:
Access+ zzgl. VLAN-Management, kryptografisches Fingerprinting, Schutz vor Layer-2-Angriffen, Gäste-System mit Selbstregistrierung

DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de