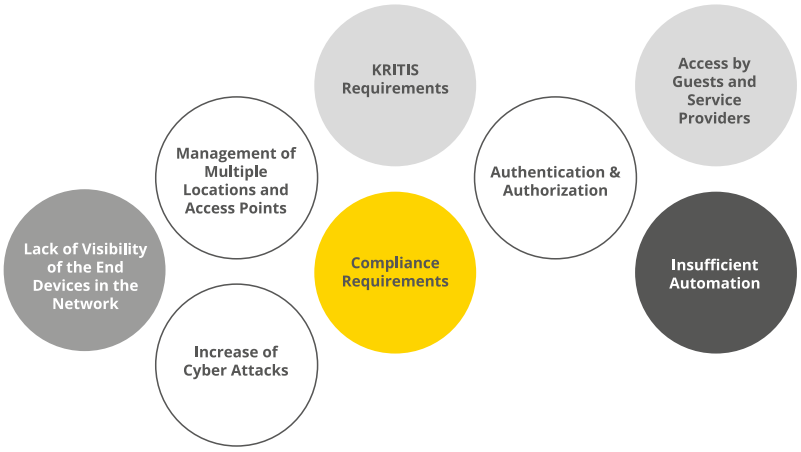
DTS

DTS
Network Access Control (NAC)

Network Access Control (NAC)

Company networks are expected not only to be constantly available, but also to provide end-to-end security. But how do you ensure precise overview, detection and control? ARP-GUARD is the leading Network Access Control (NAC) solution from the specialists at ISL Internet Sicherheitslösungen GmbH. ISL is a recognized German software manufacturer with a focus on NAC. In contrast to complex and expensive applications, ARP-GUARD is easy to implement in large, heterogeneous networks. The solution sets new standards here. It quickly and uniquely identifies all known and unknown devices, regardless of manufacturer or technology, before they are granted network access. In addition, ARP-GUARD brings together security-related information and detects, reports and corrects anomalies in the network.

- Device recognition & inventory
- Unique fingerprinting for unique device identification
- Maximum network visibility, control & monitoring
- Network segmentation & integrity down to end devices
- Vulnerability identification
- Real-time centralized policy definition & enforcement
- Protection of sensitive data & areas as well as compliance compliant data security
- Effort & cost reduction through automation
- IT security „Made in Germany“ by DTS



A common requirement of BSI, CRITIS and industry-specific institutions is that only authorized systems are allowed on the network. The most important thing here is the motto: “security comes from visibility”. ARP-GUARD detects and inventories the entire network infrastructure within a very short period. Every end device becomes visible and sources of interference can be localized. In addition, the solution provides a graphical representation of the entire architecture. This not only facilitates network planning. It provides the transparency that is required by audits and inspections, for example.

Centralized control of all network access provides comprehensive access protection. Unknown devices and status changes are detected and reported in real time. Once uniquely identified, any action can then be defined and managed by rules – from port disconnection to relocation to a dedicated Virtual Local Area Network (VLAN).

With VLAN management, network segmentation in VLANs is easy to carry out. Sensitive areas thus have additional protection, public areas are clearly demarcated from internal ones and guests and service providers are only given special access. Assignment to the relevant VLAN is automated.

The combination of different authentications, including MAC-based RADIUS and 802.1X, provides a high level of security. These methods are supplemented by ARP-GUARD fingerprinting. This uniquely identifies devices using various properties such as cryptographic certificates and keys.

Thanks to the special sensor management architecture, ARP-GUARD is multi-client capable and enormously scalable. This allows integration of any number of locations. Umbrella management enables administration of large, decentralized network environments. A central set of rules is spread over the entire network like an umbrella, easily and automatically. Users, roles, rights and policies are synchronized.

The captive portal controls the network access of guest and third-party components. In each environment, targeted access can be defined for third-party devices and controlled at all times by dynamic firewall rules, even across sites. This makes Bring Your Own Device (BYOD) easy to implement, and private devices are given explicitly authorized access.

The endpoint add-on provides valuable compliance support. During authentication, endpoints are checked to ensure they meet security policies and are compliant, including status, antivirus and patch level of the operating system. If the rules are not met, the device is isolated and can be updated in a quarantine VLAN, for example.

ARP-GUARD is used in all areas. In addition to industry, commerce, healthcare, government, education and research, the solution is now a cornerstone in the financial sector, one of the most security-sensitive industries of all.

ARP-GUARD management is provided as a virtual and physical appliance. Integration into the existing infrastructure is seamless. In a cluster installation, there is also the option of mixed operation. In addition, sensors can be installed directly on the company's own servers.

Unsere 4 ARP-GUARD Pakete:

ARP-GUARD Access – Netzwerkzugangsschutz:
RADIUS / 802.1X / EAP with and without certificate, MAC-based RADIUS, MAC authentication, user-defined rules, central dynamic port security system, guest system with self-registration

ARP-GUARD Access+ – NAC & VLAN-Management:
Access plus demarcation of network segments, dynamic and static allocation, cryptographic fingerprinting, guest system with self-registration

ARP-GUARD Finance – Layer 2 IPS & NAC:
Access plus protection against layer 2 attacks, protection against foreign and unknown devices, cryptographic fingerprinting, guest system with self-registration

ARP-GUARD Premium – All in One:
Access+ plus VLAN management, cryptographic fingerprinting, protection against layer 2 attacks, guest system with self-registration

DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de