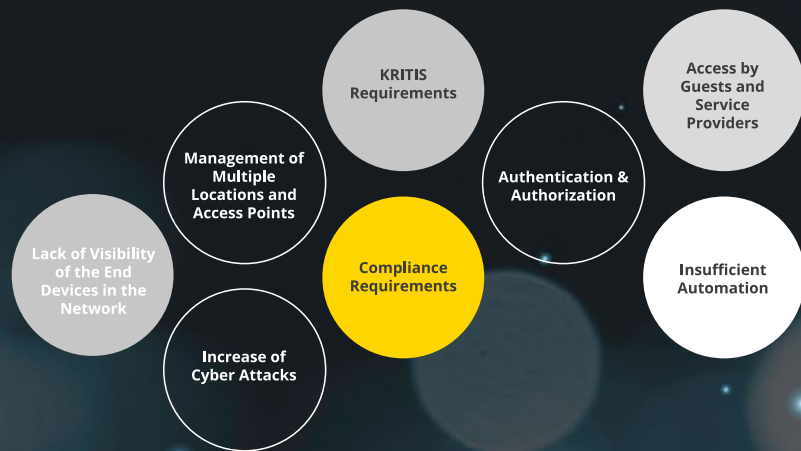




# DTS NETWORK ACCESS CONTROL (NAC)

Continuous availability and security of corporate networks - both are now expected as standard. But how can you ensure precise visibility, detection, and control? ARP-GUARD, developed by ISL Internet Sicherheitslösungen GmbH, is the leading Network Access Control (NAC) solution. ISL is a recognized German software company specializing in network security. In contrast to complex and costly applications, ARP-GUARD can be easily implemented in heterogeneous and large networks and sets new standards. It quickly and accurately identifies all known and unknown devices, regardless of manufacturer and technology, before they gain access to the network. In addition, ARP-GUARD consolidates security-relevant information and detects, reports and rectifies anomalies in the network.



Regulations and industry-specific institutions have a common requirement: only authorized systems may access the network. The central principle here is: "Security through visibility". ARP-GUARD detects and inventories the entire network infrastructure in a short time, makes every device visible and identifies sources of interference. The solution also provides a visual representation of the entire architecture, which simplifies network planning and creates the necessary transparency for audits and reviews.

Centralized management of all network access points ensures comprehensive access protection. Unknown devices and status changes are detected and reported in real-time. After precise identification, actions can be defined and managed through rule-based protocols — from port shutdown to placement in a specific Virtual Local Area Network (VLAN).

With VLAN management, network segmentation into VLANs is easily implemented. Sensitive areas are given extra protection, public zones are clearly separated from internal ones, and guest or vendor access is granted only as needed. VLAN assignments are automated.

The combination of various authentication methods, including MAC-based RADIUS and 802.1X, offers robust security. These methods are enhanced by ARP-GUARD fingerprinting, which uniquely identifies devices using characteristics like cryptographic certificates and keys.



ARP-GUARD's specialized sensor management architecture is multi-tenant capable and highly scalable, allowing for the integration of numerous locations. The enterprise management feature facilitates the administration of large, decentralized network environments. A centralized rule set spans the entire network like an umbrella—simple and automated. Users, roles, rights, and policies are synchronized seamlessly.

The captive portal regulates network access for guest and external devices. In any environment, specific access for external devices can be defined, continuously monitored by a dynamic firewall rule set, even across multiple locations. This makes implementing Bring Your Own Device (BYOD) straightforward, with private devices granted explicitly authorized access.

The agentless endpoint extension provides valuable compliance support. During authentication, it verifies whether devices comply with security policies, such as OS status, antivirus, or patch levels. If policies aren't met, the device is isolated and, for example, updated within a quarantine VLAN.

ARP-GUARD is used across all sectors. In addition to industries like healthcare, government, education, and research, the solution is indispensable in the financial sector, one of the most security-sensitive industries.

The ARP-GUARD management platform is available as both a virtual and physical appliance, integrating seamlessly into existing infrastructures. In a clustered setup, a mixed operating mode is also an option. Sensors can also be installed directly on company servers.

- device detection & inventory management
- Unique fingerprinting for precise device identification
- Maximum visibility, control & network monitoring
- Vulnerability identification
- Centralized real-time policy definition & enforcement
- Protection of sensitive data & areas, ensuring compliance with data security standards
- Reduced effort & costs through automation
- IT security „Made in Germany“ by DTS
- Also available as NAC as a Service

## NETWORK ACCESS CONTROL AS A SERVICE (NACAAS)

With ARP-GUARD NACaaS, you get comprehensive network protection without burdening your own IT resources. Your IT department can be supported 24/7 by our network specialists, eliminating the need for expensive in-house experts. There are no high upfront costs, and

pricing remains transparent. Regular updates and maintenance ensure optimal operation of our solution. Additionally, the service can be flexibly adapted to growing or changing network environments to meet your evolving needs.

