ARP GUARD by ISL

WHITEPAPER

# ZERO-TRUST
Network Access

SecurITy made in Germany

Trust Seal
www.teletrust.de/itsmig

## TRUST IS GOOD - BUT ZERO-TRUST IS BETTER

### A RESILIENT IT SECURITY CONCEPT

In traditional security models, the potential attacker is usually assumed to come from outside the network's own boundaries. This assumption ignores the increasing number of security vulnerabilities caused by components or access rights within the network. Security strategies that mainly secure companies against access from outside are not armed against the current challenges of cybercrime such as social engineering and phishing attacks. The increase in attacks launched from within the network need a further layer of protection. A holistic and resilient security concepts is required to react in a targeted manner to the existing security threats.

### ZERO-TRUST NETWORK ACCESS

Already since 2003, ISL GmbH has been pursuing with the ARP-GUARD Network Access Control solution a fundamental security approach of increasing importance for today. The ARP-GUARD NAC solution relies on the constant control of all access points and the unique identification of each device before it gains access to the network and company resources - an approach that is now widely known as „Zero-Trust Network Access (ZTNA)".

### NEVER TRUST - ALWAYS VERIFY

According to this basic principle of an advanced security concept, no device is trusted by default, even if it is within the network. Every attempt to access is consistently checked and logged - access is only granted after successful authentication. ARP-GUARD NAC provides you with essential elements for a resilient zero-trust concept at the device and network level, which can be easily expanded step by step with further functions and modules.

Maximum transparency for maximum threat protection. ARP-GUARD provides an instant and complete overview of all assets on the network.

ARP-GUARD offers a comprehensive set of rules in which you can set company-wide and user-defined policies. Control which resources are accessible to whom and protect sensitive data and resources from unauthorised access.

By continuously monitoring network activity, ARP-GUARD provides an overview of everything that is happening in your network in real time. Unwanted access and conspicuous deviations can be identified at an early stage and the security level in your network is significantly increased.

The micro-segmentation of the network prevents potential attacker from moving freely in the network. The spread and the damage caused by attacks are thus drastically reduced and more controllable. The ARP-GUARD VLAN management allocates the devices dynamically and according to granual security guidelines for the various segments in the network defined in the set of rules.

ARP-GUARD Endpoint checks whether the device meets the company demands such as compliance or security requirements in the network before accessing the network.

ARP-GUARD uniquely identifies each device before it gains access to the network. The strong authentication through fingerprinting protects against network manipulation such as MAC spoofing or ARP poisoning.

**How To Explain Zero Trust To Business Executives?**

Building an architecture that "never trusts, always verifies" connections and that assumes a bad actor is active at all times leads to highly resilient, highly flexible environments that are much better suited to the demands of the modern workplace.

*Source: www.gartner.com*